# **Automotive Cybersecurity Risk Assessment**

# What is this, when and why is it needed?

The first time we encounter a cybersecurity risk assessment is at the very first stage of a vehicle’s lifecycle. When a new vehicle is being designed, in accordance with the upcoming ISO/SAE 21434 Standard – “Road vehicles – Cybersecurity engineering”, automotive manufacturers need to perform an initial cybersecurity risk assessment – a Cybersecurity Risk Audit.

Equipped with the audit results, we can eventually define our cybersecurity goals, and refine our cybersecurity requirements, which leads to a cyber-secured design.

However, as I have explained in a previous blog (LINK), this is just the first out of many times in which we conduct the process. This routine, which is not yet fully operational in the automotive industry, is, nevertheless the one which is initiated when a new alert appears in your automotive Security Operation Center – as it is part of the incident response procedure.

Suppose for example, that one of the following incidents has occurred:

* an attack has just been identified in one of your vehicles on the road, or
* a new CVE is published online, which may potentially affect one of your car models.

Using the results of the risk assessment, the manufacturer then creates a cybersecurity incident response plan, conducts required maintenance if needed, and hopefully returns to a secured state.

# What are the requirements from this process, or what should it provide?

A robust risk assessment process provides insights that enable us to take a practical and pragmatic decision – clearly not every vulnerability publication should force us to issue a recall, or deploy a patch by means of an OTA software update. Having made a correct and mature impact assessment, we are able to make a more courageous, yet not naïve, decision.

However, diving deep into one’s environment can be a time-consuming process, and the search for a smart assessment can take time if done incorrectly. One wants the process to be fast enough to be able to identify the critical issues as soon as possible, and provide immediate treatment if needed. In addition, such a process should be almost automatic so as to be able to handle the stream of incidents that will be flowing into automotive SOCs (Security Operations Centers) in the not too distant future.

# How? The technical discussion

Let us suppose that a new alert has just popped up in our bright and shiny automotive SOC, which originated either from one of our already-deployed on-board defense solutions, or alternatively a vulnerability has been published as-is.

How can we achieve the best risk assessment process? The new ISO/SAE 21434 Standard suggests a roadmap for such a process.

Breaking this down and translating it into language that is easier to understand:

Asset identification – or, am I affected? and if so, where?

The first step is **exposure** assessment. We need to identify whether we have any assets that could be potentially affected by the said vulnerability or attack. These assets could vary from Binaries, MCUs (microcontrollers) and Networks to PII (Personally Identifiable Information).

Following asset identification, we then need to map them and consider:

* what other assets could they affect? For example, one Binary could potentially be deployed on multiple MCUs, thereby increasing exposure more than expected.
* on which car models do those (now) risky assets reside?

TO DO: add arrows from left to right to show conclusion process

Currently, the data required to conduct an accurate asset identification may be scattered among the OEM and its various suppliers, so that the complete hardware and software BOM (Bill of Materials) might have to be checked. This means that upon the occurrence of any type of incident, the OEM will need to approach its suppliers to query them about the existence of the affected asset.

Such process will necessarily be very expensive, requiring man more involved parties, in addition to the SLA and natural round-trip delay between OEM and supplier. To comply with the process requirements defined above, OEMs need to own this data from the outset, thereby having a clear visibility of their own assets.

Vulnerability analysis and threat scenarios – or, what can the attacker do?

If we assume that we have been affected, then our next task will be to understand what the attacker can do with such a vulnerability or attack vector. We need to investigate what opportunities or possibilities the attacker will face when trying to exploit the said vulnerability.

For example, the attacker could be leveraging their proximity to target vehicles with a published Remote Code Execution vulnerability to penetrate the vehicle from a non-secured or monitored network, allowing easier lateral movement in the following steps and a direct route to safety ECUs.

A simpler case might need to assume that the attacker has already gained access to one of the vehicle’s internal components, and the said attack vector would thus allow them to send a malicious command to the safety ECU.

Basically, we need to “play” the role of attacker in our own network, taking into account its complete topology, endpoint characteristics, and the various security measure we have deployed.

Risk determination – taking both factors into account

Once the complete threat model is in place, we need to conclude what the risk level of the incident will be..

We need to consider two parameters which together comprise the risk determination:

1. the feasibility of attack – what are the [practical] chances that this incident will [re-] occur.
2. Impact Rating – if such an incident does actually occur, what will be its impact – is it a safety issue? or perhaps “just” a financial issue such as locking down the vehicle ahead of usage and thereby preventing its usage, an example perhaps of ransomware.

Let’s look at two examples:

1. a relatively simple case – namely that of Bluetooth vulnerability.
A Zero-Day vulnerability has just been discovered in a popular embedded Bluetooth stack. The vulnerability severity score is high, enabling Remote Code Execution with no Privilege Escalation required to follow, and physical proximity is required to exploit the vulnerability.

We first realized which of the car models we released to market (and also planned future releases...) actually contain this popular Bluetooth module – which is probably installed on some perimeter system such as an IVI or TCU. For the sake of discussion let us assume that the affected device, our asset, is the TCU.
Secondly, we researched the possible attack vectors and attacker’s mode of operation.
Now, let’s take a closer look at three possible scenarios:

* 1. The asset is protected by an embedded security solution that prevents exploitation of the vulnerability.

GW

TCU

ECU

ECU

Safety ECU

Gateway

* 1. The asset is protected by a peripheral security solution that prevents any further movement from the exploited device into the vehicle’s internal systems.



GW

TCU

ECU

ECU

Safety ECU

Gateway

* 1. The asset is not protected by a security solution, and provides a path straight into the vehicle’s safety networks.

GW

TCU

ECU

ECU

Safety ECU

Gateway

And the list goes on …
Each of these scenarios might have a similar feasibility of occurrence, yet their impact might be completely different, ranging from zero impact to a full spectrum of safety implications.

1. a more “complex” case - AUTOSAR vulnerability

Consider the case where a Zero-Day vulnerability has just been published, affecting a popular AUTOSAR implementation. The vulnerability severity score is high, enabling Remote Code Execution with no Privilege Escalation required to follow, and same-network accessibility is required to exploit the vulnerability.

We quickly established what the affected ECUs were, and accordingly the relevant car models, following a listing of possible attack vectors. For the sake of discussion let us assume that the asset is a safety ECU residing two legs from the vehicle perimeter.

Again, let us take a closer look at three possible scenarios:

* 1. The asset is protected by an embedded security solution that prevents exploitation of the vulnerability.



GW

TCU

ECU

ECU

Safety ECU

Gateway

Safety DC

* 1. Each of the routing ECUs on the way from the perimeter to the asset has a Network IDPS which manages and monitors inbound packets.



GW

TCU

ECU

ECU

Safety ECU

Gateway

Safety DC

* 1. The asset is not protected by any security solution, and there exists an unprotected network path from the perimeter to the asset.

GW

TCU

ECU

ECU

Safety ECU

Gateway

Safety DC

And the list goes on…
Each of these scenarios may have a similar safety impact if the vulnerability is exploited, however the feasibility for exploitation varies widely, ranging from:

1. Minimal feasibility – which assumes that the attacker has already bypassed several security measures, and could potentially harm other devices on the way to our asset.
2. High feasibility – assuming there is another publicly-vulnerable device on the perimeter and direct path from this to our asset.

We understand that the risk is a function of two dominant factors – Attack Feasibility, and Impact Rating. Each could have a completely different effect under different circumstances.

Once the risk level is determined, and taken into account, we can finally conclude what threat it is that we are facing, and can then make a more ‘mature’ decision on how we should react.

Risk Treatment (management)

Deciding on the course of treatment might seem trivial after following our thorough process and finding the sought-after “smart” risk determination. However, such a decision also takes into account the supply-chain constraints, various car programs and variants in sub-models.

We also need to ensure that our treatment does not interfere with other much-needed cybersecurity policies or tough decisions already made regarding the affected vehicles.

Any treatment should be well-instrumented, tightly-monitored and verified across all affected models, just like any other treatment carried out in the automotive industry.

# Time is of the essence

Cybersecurity risk assessment is not a non-recurring process, but is unfortunately a quite frequent one that we will be faced with involving various events from multiple sources. As we see automotive attacks increase with time, we can expect to deal with more and more incidents which will require our attention and resources. We, therefore, have to react much more rapidly as an incident can easily get out of control while we are still assessing the risk. Such incidents cannot be handled in a classic automotive timeframe.

The risk assessment process should be completely streamlined, reducing the time from weeks, as is the case today, down to days and even hours in the near future. Preparation is key to success – to enable such a process, the assessor must gather all the required data ahead of time so as to support the different steps needed.
When handling a potentially devastating incident, the assessor cannot allow him- or her-self time-wasting SLAs with the various entities related to the process.

# Who? the OEM

Using the various scenarios and possibilities that we have analyzed, we have only scratched the surface. It should be clear that sometimes to properly perform risk assessment, we will need the full scope of the vehicle. At the very least this requires the affected vehicle’s topology, hopefully accompanied by the relevant HW and SW BOM.

The only entity in the complex automotive supply-chain that can be responsible for this is the OEM.
Not only can this not be done by one of their suppliers, as they do not have the full scope of the vehicle, but the OEM should also strive to conduct the process with minimal intervention and delays by other parties, to avoid time-consuming round trips between the various suppliers.

# In conclusion

As the new ISO Standard indicates - manufacturers must now demonstrate how they identify new and evolving cyberthreats and vulnerabilities and how they will react appropriately.

We can now understand that risk assessment is a process that does not necessarily result in a binary result – whether 0 or 1, but is rather a more complex determination that can vary even within its own car programs.

This is also now presenting OEMs with a new requirement – namely, to quickly assess their own vehicles down to the very ECU’s HW and SW BOM, resulting in independence from supplier intervention or delays. The OEM’s key to success to deal with these new requirements is by means of timely preparation, and taking a more cyber-strategic approach towards the management of the cybersecurity lifecycle, enabling better procedures and responses so as better handle the next incident.