**The road to cyber security scoring needs transparency**

Last week, the 5stars organization published its draft of the “Roadmap to Resilience,” which describes the route to realizing cyber security scoring.

To summarize, the 5stars organization was established to meet the demand from the automotive ecosystem to understand vehicles’ cybersecurity posture. It has therefore set a goal for itself to create an NCAP cybersecurity equivalent.

Providing the end consumer with transparency, whether their car is secured or not, is a key element to create a cyber-secured ecosystem.

A recent poll published in *PC Magazine* (<https://www.pcmag.com/news/369254/whats-the-scariest-thing-about-driverless-cars-hint-its>) revealed that 45 percent of consumers reported safety concerns and technological failures being their biggest fears with autonomous vehicles. The cost of the vehicles and hacking threats took the next spots on the list with 16 percent and 15 percent of consumers reporting those concerns, respectively.

30 years ago, when the first safety ratings were published, consumers didn't care about airbags, ABS systems, or any other safety measures for that matter. Fast forward 30 years later, and no consumer would dare to purchase a car without air bags. The automotive ecosystem understands that it now needs to create a cybersecurity scoring system.

However, cybersecurity scoring might end up being a much more complicated process than the standard safety procedure.

Today, in the world of safety scoring, insurance companies investigate cars relating to several categories, including:

1. Maintenance (ongoing, post-accident auto repair, etc.)
2. Safety
3. Security – both physical and cyber.

For most of the above, in addition to other categories not listed, the tests can performed by a third party tester/auditor **independently from the OEM/manufacturer.**

Furthermore, for most of these categories, the test results **are both valid and relevant for the majority of the product’s lifetime**. In other words, a car’s safety rating, which takes into account safety measures like airbags, the ABS system, etc. mostly doesn’t change throughout the car’s lifetime.

However, one score stands out: that of cybersecurity. The way to realize it is quite complex and has revealed new requirements.

The draft of the “Roadmap to Resilience” paper emphasizes two main security elements that are strongly needed to realize the security scoring:

1. Security assessment (audit risk)
2. Security management throughout vehicle lifetime (ongoing risk assessment and incident handling)

Audit risk and risk assessment are the building blocks of the insurance world. In any industry, when a company decides to get cybersecurity insurance coverage, it first needs to perform an audit risk assessment. This consists of filling out a questionnaire, providing the insurer with information about the company’s overall security posture, and allowing the insurer to assess the level of protection and security applied within the company. When the coverage needed is high enough, the insurer will then request a more thorough investigation be conducted, allowing them to ensure that they have all of the required inputs to precisely assess the company’s potential cybersecurity risk. After the company security posture risk is calculated, then an insurance policy will result with specific terms. Later, when requesting to renew the policy, the client will need to report any deviations or changes from what they indicated on the original questionnaire, in addition to reporting any incidents that occurred and their impacts. Sometimes, the company may even need fill out the questionnaire from scratch again. This allows the insurer to re-assess the risk and set the premium and coverage accordingly.

The problem with Automotive Cybersecurity is that the following two elements behave very differently than in other aspects of vehicular safety:

1. Testing (audit risk) – independently pentesting an entire vehicle—which today is comprised of multiple networks sometimes connected to more than 200 ECUs without any inputs from the vehicle manufacturer—is extremely expensive and time-consuming. In addition, due to the nature of sophisticated cyber-attacks, the penetration testing required to assess the vehicle’s security level is conducted at the same level as traditional safety testing, which might not be enough.
2. Relevance as a factor of time (ongoing risk assessment) - even if the auditor managed to conduct a thorough risk assessment and generate a sufficiently detailed report for a specific vehicle, the results are not going to be relevant several years or even months after production. A vehicle’s cybersecurity posture is very fluid and might worsen after the discovery of a serious vulnerability. In contrast, it could improve after a significant security update.   
   Considering a vehicle’s longevity, the first assessment will be irrelevant for the majority of the product’s lifecycle.

How do you re-assess the vehicle’s security posture during its entire lifecycle? Is it feasible?

In order to successfully and feasibly perform both an audit risk and risk assessment throughout a vehicle’s lifecycle, two things are needed:

* + - 1. OEMs must generate awareness of their car models, including the HW & SW BOM models’ architecture and topology. Such an awareness will allow for the audit risk and risk assessment processes to proceed.
      2. OEMs and their partners (insurance companies, certification institutes, etc.) must find a way to share some of their data or conclusions.

Currently, both requirements have not been widely implemented. OEMs find it difficult to generate awareness across their car models, and there is a lack of transparency between the OEMs and their partners throughout the product lifecycle with regards to cybersecurity.

Therefore, there are two sides to the equation – the auditors and the auditees.

If we want to realize cybersecurity scoring, which is definitely a common goal for both the industry and consumers, then we need to find a way to allow both sides to collaborate while still keeping everyone’s interests intact, and to provide consumers with the most accurate scoring possible.