HOW AUGMENTED SECURITY CAN HELP THE AUTOMOTIVE WORLD

The automotive industry is a big consumer of software, whether it is customer management software, inventory management software, parts design software, etc. Kompass has 107 different software packages.

As for cybercrime in the automotive industry, everyone from Kaspersky to the biggest companies like Apple, Oracle, EMC Symantec, SAP, CapGemini has been involved for a long time. You only have to read the numerous press releases that are currently being issued. Could the war in Ukraine have something to do with it? Below are excerpts from a Wikipedia article which is edifying:

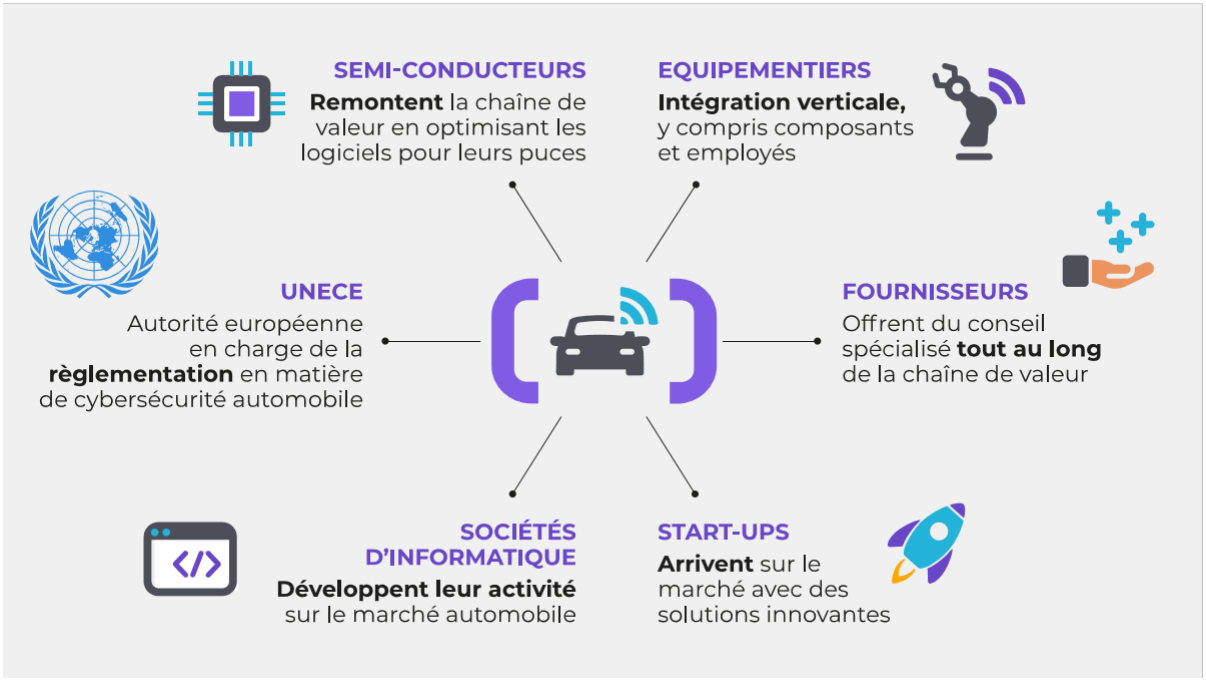
*"**Vehicle IT security** is a major challenge for modern automobiles. This issue is taken into account right from the design stage of onboard systems.*

The connected vehicle is controlled by interconnected on-board computers (ECUs). Through these ECUs, the modern vehicle offers new functionalities that improve driving quality and enhance passenger safety. However, manufacturers are confronted with computer security issues induced by devices such as ODB plugs, Bluetooth, Wi-Fi, 3G/4G, RFID, USB keys, CDs, which are very common on modern vehicles. Each of these devices could be an open door for hackers wishing to access the various on-board computers.

*In 2015, American researchers Chris Valasek **(en)** and Charlie Miller exploit the vulnerability of the multimedia system and take control of safety and comfort functions (brakes, steering wheel, engine power, windshield wipers) and entertainment (car radio volume). This demonstration from a remote external computer highlights the security weaknesses of in-vehicle applications. These devices are responsible for exchanging information between the vehicle and/or the driver and the manufacturer's computer system as well as for the authentication process and the encryption of the onboard codes.*

To anticipate and avoid these cyber attacks, the connected and/or autonomous vehicle industry and equipment manufacturers are increasingly partnering with security specialists to find solutions or countermeasures. The economic, technological and societal stakes are commensurate with this challenge.

Source The automobile, the latest defi in cybersecurity?



All of them put forward proprietary architectures that secure communications and processes between the vehicle (from cars to trucks, buses and of course military vehicles) to the cloud and/or their proprietary communication systems.

To simplify, there are three cybersecurity standards

- WP29 U
- UN 155 "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system " *This is the standard used by UTAC.*
- ENISA 2019

These standards help to make vehicles safe from their construction to their use.
Both to secure the behavior but also the construction.

However, these new standards that these partners are putting in place do not concern the confirmation by the driver that his vehicle is connected to the Internet.

Also, except for one of them, these standards are not approved by UTAC[1] which is the almost official automotive laboratory. It is the recognized authority that validates all automotive procedures and vehicles. In other words, it is good that the automotive world is making the engine/vehicle/communication environment safe, but these safety intentions do not seem to take into account the importance of involving the user, whoever he may be.

However, the application of these cybersecurity standards cannot be done without the agreement of the last link: the driver in the broad sense. This risks creating a misunderstanding on their part: "*once again, something is being hidden from us",* except that it is not pollution, it is the very control of the vehicle. And except that in some cases it has existed for 10 years without being announced.

Let's think positively: we deprive this last link, the driver, of a strong information: he is protected against external aggressions.

Especially since European laws require that interactions meet the PSD2 standard. "In the area of security features, the most sensitive element of PSD2 is the generalization of multi-factor authentication (MFA) for certain operations, including online payments.

It seems normal, then, given the price of these vehicles that the DSP2 standard applies to them.

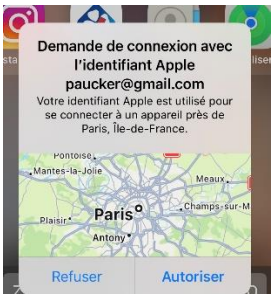
What does this standard actually do? It forces to ask a second validation agreement to a buyer (in our case a driver). An electronic GTC in a way. In other words, it is normal to protect a vehicle, but the driver must be aware of this and agree to it. Otherwise, scandals like VWgate will appear when journalists or consumer organizations become aware of the opacity of the manufacturers.

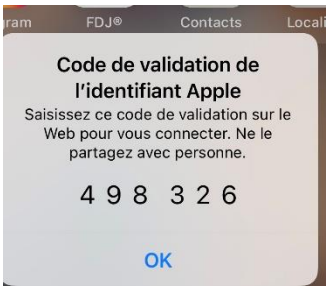
How do double signatures work, for the most part

[1] UTAC = **Union technique de l'automobile du motocycle et du cycle**, is a private organization, controlled and financed mainly by the French automotive industry

Regarding this act of validation, legal double signature or strong authentication, there are protections put in place by the market.

For example, at Apple you receive a first message to verify that it is you who is requesting the connection followed by a code that you must copy on the transaction in progress or simply open a software (photoshop for example). It's a bit heavy.





Today the vast majority of such systems work with the sending of a code by SMS.

An SMS is hackable and the only protection is the validity of the SMS which is on average less than 10 minutes. This explains the number of failed transactions. It is necessary to juggle between two windows of the same terminal or to juggle with two distinct screens PC and smartphone. Then this code must be retranscribed on the transaction itself, without error while the number of characters tends to grow.

In general the existing systems :

- Run on the cloud so no local control
- American sources. No control and no certainty that the system is really opaque

In conclusion, the double signature or reinforced signature in most cases remains hackable today and it is a rather complex process because it requires to carry over without making mistakes codes all unique and difficult to remember.

What makes us unique

Augmented Security's patent facilitates agreement on the triggering of cybersecurity protections by reversing the request for proof.
Current procedure: the manufacturer sends a different code by SMS each time the driver has to retype on a keyboard

Augmented Security procedure: the driver only has to type in the password he has chosen, which is easy to remember and is implanted in the space secured by Augmented Security.
This code will always be the same for each request since the security is provided by the software environment and not by a hackable code sent by a non-secure SMSM.

An example: the Augmented Security procedure can be translated by a message displayed on one of the vehicle's screens "*Do you agree to be connected to our cybersecurity*" followed by a space where the driver will type in his or her code of 4 to 6 digits, known only to him or her, on a virtual keyboard that will be displayed. Of course, this can also be used to start the vehicle.

Saving time but also simplifying procedures for drivers. Experience has shown that the more complex the procedure, the greater the chances of it being circumvented.

In conclusion, Augmented Security proposes a patented interface between the vehicle and the manufacturer that will trigger cybersecurity activities with the driver's consent.
Augmented Security performs this function in
a quick and easy way. To our knowledge there is no equivalent procedure:

- European Patent
- We own 100% of our code, our sources.
- Horizontal, cross-platform solution
- Integration with manufacturer solutions.
- Double signatures 100% secure, which is not the case of many current procedures using SMS that are "hackable".
- Strong security of the terminals used but also of the servers creating a continuum on the whole chain from the transmitter to the receiver.
-

In conclusion, Augmented Security offers a true Strong Authentication, which will give drivers control over their vehicles' communications, a function that will be developed further.