WHITE PAPER

INSIGHTS FROM CONNECTED MOBILITY

Maintaining Data Protection and Security for the Connected Car

Software updates over the air – handling security gaps ahead of time!

DR. HOLGER HILMER
Senior Engineer Technology Research

CONSUMER DEVICE INTEGRATION

molex

WHITE PAPER

INSIGHTS FROM CONNECTED MOBILITY

Maintaining Data Protection and Security for the Connected Car

Software updates over the air – handling security gaps ahead of time!

INTRODUCTION

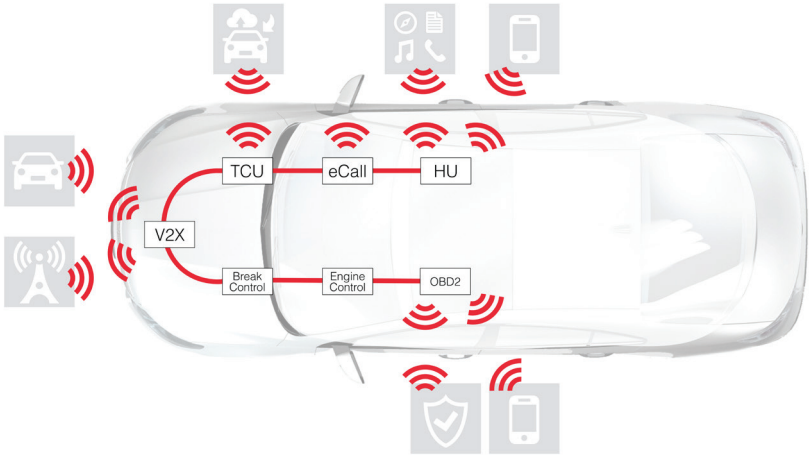
Recently, many hacker attacks on connected cars have made a great stir and challenged the security of such systems. Usually, a wireless connection was used to gain access to the CAN bus, which interconnects many control units within the vehicle. In this way, remote control was achieved over the brakes, the acceleration, the door lock, the air-conditioning system, the wipers and other functions.

In recent times, car hackings such as these have regularly made headlines. This is not particularly surprising, because more and more vehicles already have their own interfaces to exchange data externally.

The vehicle becomes a mobile living space; cars develop to be mobile devices. Especially from younger customers, there is a rising demand for convenience functions so as to remain interconnected, or to share vehicle data such as consumption or power output via apps and have them evaluated.

So the connected car has already become a reality. It is a subject not just electrifying customers and manufacturers, but also security researchers and IT experts. And in a worst case scenario, criminal hackers as well. For years, security experts have observed the fact that the desktop PC is not the only target of digital attacks anymore. A large part of the malware is now customized to hit mobile devices. It would be negligent to believe that this development would leave the connected car unmolested.

So far, attacks of criminal hackers on vehicles and their systems have been very rare exceptions. But the pivotal importance of security for connected cars has clearly become apparent to the OEMs by now. When the vehicle becomes a personal mobile device used by its owner for communication, and possibly personalized by apps, this set-up provides would-be assailants with a multiple potential of manipulations.



Software updates over the air maintain security

But how can the automotive industry protect itself and its customers against digital attacks? Ruling out all air interfaces, a concept long favored by parts of the auto industry, is not in the interest of the customer. The need of a data exchange connection is also evident with innovative V2V or V2I services that will be developed, including their relation to autonomous driving. So for the future, there is no way to entirely avoid Bluetooth, WLAN or Cellular in the vehicle.

On the other hand, the classical approach – using call-backs and remedial work in repair shops – will not provide timely success in safeguarding vehicles against digital assailants either. In addition, recall campaigns cause tremendous expenses and damage the reputation of the car manufacturer.

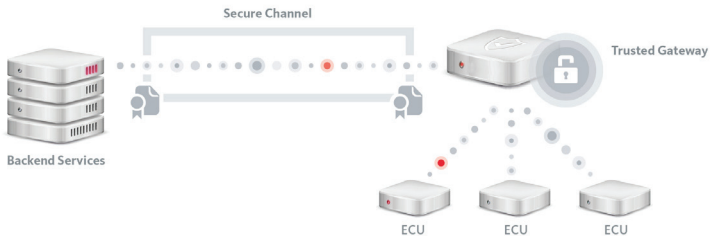
The race against car hackers cannot be won in this fashion. After all, it takes months before all jeopardized vehicles will have received a patch this way. In the meantime, hackers would continue their mischief. But such a time frame to ward off the danger is unacceptable, because a manipulated vehicle can pose an enormous risk to the driver as well as his environment. Moreover, in many cases it is possible to identify further weaknesses in the vehicle software during such a period. So the patch is already obsolete at the time of its installation.

So let us take a look at the world of mobile devices, to find an indication of the alternative to repair recalls: The suppliers of apps and smartphone operating systems constantly deliver up-to-date versions of their products to terminal devices. Sometimes it is a matter of small patches to address weak spots, while in other cases new versions including new functions are launched into the market.

Such updates of software and firmware are delivered "over the air (OTA)", i.e. by way of air interfaces. As soon as these updates have been transmitted to the device, they are extracted and installed automatically.

Firmware over the air (FOTA) is an answer to the challenges of swiftly equipping a multitude of devices with the latest updates. The update procedure provides the potential of swift and continuous remedy of weak spots with appropriate patches, at the same time integrating new functions and modernizing cryptographic methods to secure, for example, the control units.

To make sure that a large number of control units can be updated by FOTA, the gateway method is employed. Between the back-end and the control units to be updated, one control unit equipped with a mobile radio interface assumes the role of an intermediary. It receives all software packages through the air interface and distributes these to the destination devices via CAN bus systems or more performant communication channels such as Ethernet. In addition, the gateway ECU has the master function in controlling and coordinating the whole updating process. If an error occurs, for example, rollback mechanisms may have to be initiated.



A paradigm change

Apart from the possibility of closing security gaps by FOTA, many other technical measures, of course, are necessary on the device side, such as cryptographical safeguarding of all ECU interfaces, especially the wireless accesses for mobile communications, Bluetooth and WLAN.

In addition, the organization and the development processes will also need to be adapted to the new circumstances. For example, end-to-end risk analyses are not the rule – but by now, they should be a mandatory part of the requirements asserted by manufacturers toward their suppliers. In this endeavor, possible scenarios of attack upon any and all components of the chain would be scrutinized, including their effects on security and ultimately on functional safety. Based on the results, adequate protective measures can be taken. Any success in this approach would only be guaranteed if the OEM, the supplier of the back-end solution and the control unit manufacturers co-operate from an early stage of development forward.

This approach requires turning away from the black-box development of control units, rather to embrace a holistic approach to security. Moreover, measures to generate and maintain security must not be terminated after production has begun. Security analyses, security-oriented testing and the remedy of security gaps by FOTA must be kept up continuously throughout the lifespan of any product.

Organizational measures concerning secure development and production include, for example, controlling the means of access to confidential data, such as keys and certificates, as well as development specifications related to components relevant to security. Such data and documents must be stored in an encrypted form on safeguarded servers, access to which is limited to very few persons by means of authentication.

Special importance must also be assigned to security-oriented testing. Penetration tests, in particular, make it possible to pin-point security gaps. Using the means and methods of hackers, the tester will deliberately try to intrude into the system. The results indicate the current level of security and will inform the development of counter-measures to seal off critical weak spots.

Technical challenges

Taking a look at the FOTA process chain and the functional units involved, you will get an idea of the complexity and the advanced technical requirements.

In this, security has the highest priority. We must have a guarantee that the FOTA process itself is safe to accomplish, without being subject to any additional attack potential. If FOTA could be abused to wrongfully introduce manipulated software into a device, the consequences in terms of security and ultimately even functional safety might be incalculable.

Cryptographical safeguarding of the air interface is one of the prerequisites for a safe FOTA mechanism. It is common practice to establish a safe connection by means of the TLS protocol. The keys and certificates required for this must be introduced into the devices in a manner maintaining secrecy and safety against manipulation, to be stored there in a safeguarded storage area. A dedicated Hardware Security Module (HSM) is indispensable in bringing about a safe storage and securely performing cryptographic procedures.

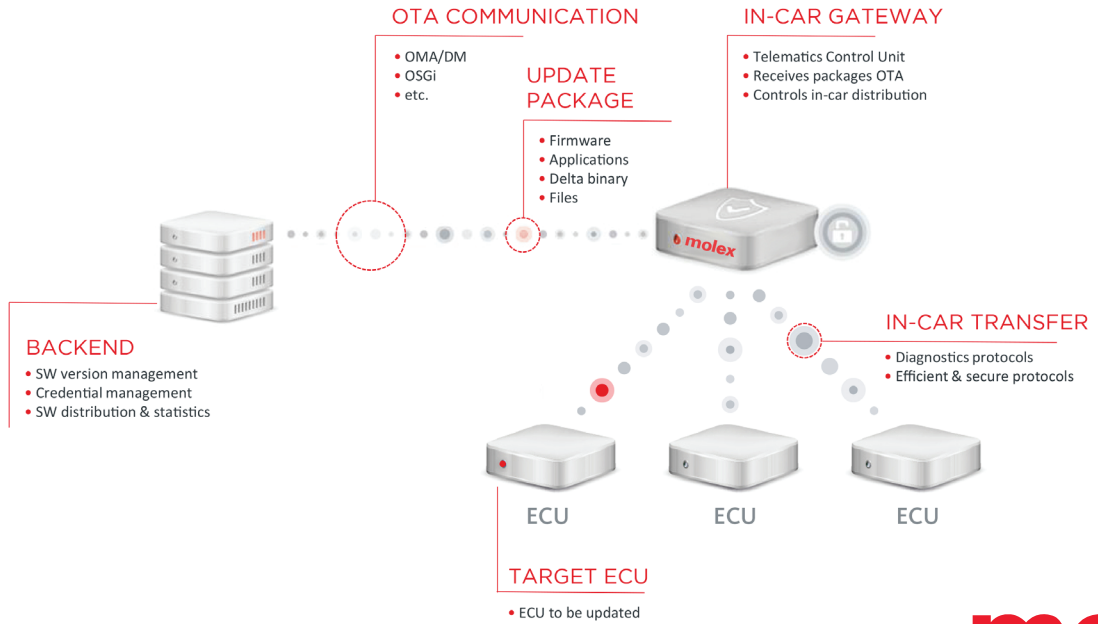
A safeguard against wrongful installation of manipulated software is achieved by using a safe installation process (Secure Flashing) as well as the security-oriented inspection on starting up the device software (Trusted Boot). In either mechanism, digital signatures are used to validate the authenticity of the software.

Development interfaces such as UART, USB or JTAG must either be deactivated in the serial product or safeguarded by cryptographical procedures, in order to prevent intrusion into the device. Through this channel, assailants might try to read out or manipulate the software or confidential data.

In addition to safe execution of the FOTA process, fast and efficient handling should be sought. On the one hand, the volume of mobile communication data and thus the cost should be minimized. On the other hand, the owner of the vehicle should be impeded as little as possible.

Efficient handling is achieved by incremental updates. In this procedure, only the changes to already installed software are transferred and installed on a binary or file basis. The delta algorithm used and the software partitioning into static and changeable data areas have a significant influence upon the size of the data packets.

The FOTA process must be very robust and fault-tolerant in order to prevent the installation of incompatible, corrupt or inconsistent software resulting in impaired functionality. In this context, identification of errors through integrity inspections as well as the supervision of the communication channels have great importance. On error, appropriate responses are required, e.g. by way of rollback actions that re-establish an error-free state.



The Telematics Control Unit as a FOTA gateway

From a technical perspective, any control unit equipped with mobile radio can function as the FOTA gateway. The Telematics Control Unit (TCU), however, is better-equipped for this task than other units. The head unit, for instance, is an integral part of many vehicles, too, and additionally it has sufficient storage space and processing power. However, most head units include numerous wireless interfaces.

This unit, after all, is supposed to be addressed by external sources via Bluetooth, WiFi or NFC, with a multitude of requirements. This fundamental openness to the outside world impedes effective safeguarding against manipulations.

Moreover, the fact that it is installed directly at the dashboard rather precludes defining the head unit as the central FOTA gateway. After all, hackers might also have rather easy physical access here.

The physical location of the TCU, however, lies deeper in the vehicle and would be difficult to access from the interior of the vehicle. All in all, it has fewer connections, and in addition, these can be deactivated when the need arises.

Also, many other security-critical functions are already represented in the TCU as of this date, such as remote activation of the immobilizer. Due to these security-critical functions, the security measures established for the TCU, such as encoding and authentication with the back-end, are a matter of course. The TCU, after all, has already become a well-established component of the security topology as used by the manufacturers.

This is an advantage because we need holistic solutions if vehicles are to be secured. The back-end, the air interface, the gateway, the vehicle bus and each control unit are parts of the chain. If the weakest part of the chain can be attacked, the safety of all other units is breached as well.

Projects where the TCU is at the center of a FOTA architecture do not just enjoy the advantage that this component is very soundly matured, judging from a security perspective. Rather, even in terms of manufacturing, suppliers and OEMs are relatively well-experienced in designing secure processes.

Further added value in FOTA

Security concerns are not the only reason why establishing FOTA via the TCU offers enormous potential to OEMs.

Expensive recalls, unpopular with customers due to cost and effort, will no longer be the inevitable consequence when weak spots show up in the vehicle – at least when dealing with software-related problems. Many problems can actually be solved without requiring any action on the part of the customer. As soon as patches can reach the vehicle on a wireless basis, the remedy of numerous types of weak spots in the vehicle will no longer necessitate any physical contact.

And in establishing new business models and customer relations, FOTA can also play a very supportive role. This is evidenced by the example of U.S. auto manufacturer Tesla.

An update offered by this company to its customers for approx. 2,000 dollars included an autopilot function. In this way, many Teslas have continued to develop into (partially) autonomous vehicles.

For OEMs, this setting opens a breathtaking new perspective. Today, it is a common situation that the value of a new car drops down to half immediately when leaving the salesman’s yard. And as time goes on, the value keeps diminishing. In the future, a vehicle might not necessarily lose value due to new functionalities as time goes on, but it might actually retain or increase its value.

So FOTA, by now, is far more than just an annoying commitment. This update procedure is not just significant because it provides basic prerequisites of effective security for connected cars. Rather, on this basis, an OEM can constantly create added value in the vehicle, ensure customer loyalty and keep revitalizing customer relations long after the original sale.

Order No. 987652-0263 Rev. 1 USA/0K/GF/2019.09