Electronic Design

By HOLGER HILMER, Senior Engineer Technology Research, Molex,
https://www.molex.com/molex/industries/connected-mobility

Close Connected-Car Security Gaps with Safe FOTA Processes

Malicious car hackings now routinely make headlines. But the rise in cyberattacks isn't surprising as more automakers incorporate wireless interfaces designed to exchange data externally. Firmware over-the-air updates can help solve the problem.

Modern vehicles have become mobile living spaces—extensions of mobile devices in homes and offices. Demand is rising, especially among younger consumers, for convenience functions to maintain and enhance connectivity, and to share and evaluate vehicle data such as consumption or power output via apps.

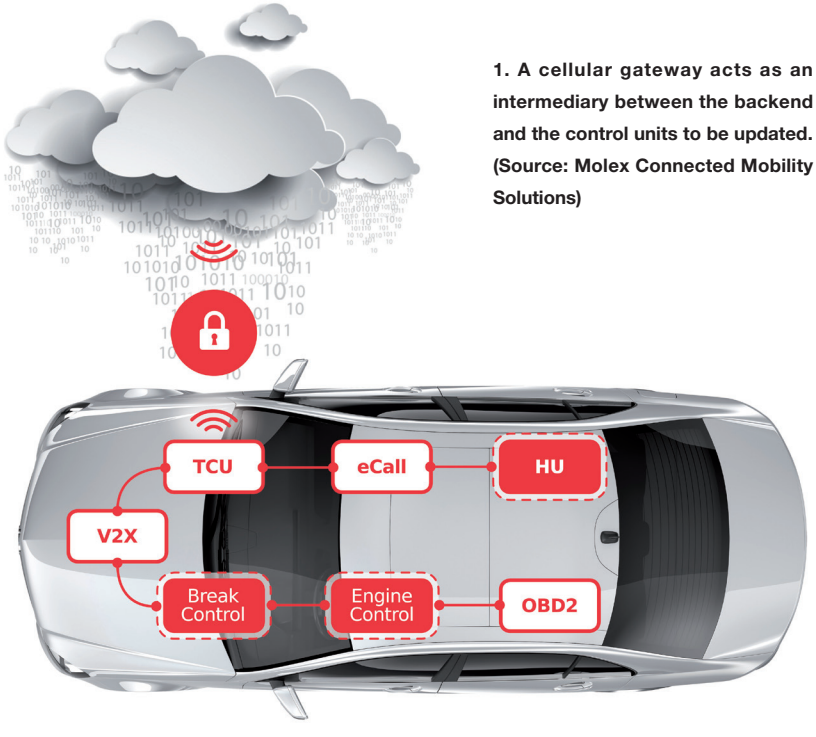
The age of the connected vehicle has become a reality. That reality excites not only customers and manufacturers, but also cybersecurity experts and white-hat hackers seeking to identify and lock down security gaps to prevent breaches by malicious actors.

For many years, security experts have observed the fact that the desktop PC isn't the only target of digital attacks. In fact, much of the malware in the mainstream is now customized to target mobile devices. It would be naïve and negligent to believe that this development would overlook the connected car.

Thus far, successful attacks by criminal hackers on vehicles and their systems represent the relatively rare exception. But the pivotal importance of security for connected cars has clearly become apparent to automakers and equipment OEMs. When the vehicle becomes a personal mobile device used by its owner for communication, and possibly personalized by apps, this setup provides would-be cyber assailants with a plethora of potential entry points and targets.

Firmware Over-the-Air (FOTA) Updates Maintain Security

But how can automakers protect customers, as well as the industry's reputation and business interests, against a rising tide of digital attacks? Eliminating all air interfaces, a concept favored by some segments within the auto industry, isn't in the best interest of drivers. The need for more data exchange



1. A cellular gateway acts as an intermediary between the backend and the control units to be updated. (Source: Molex Connected Mobility Solutions)

connections is also evident with innovative vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) services currently underway, including the development of infrastructure to enable autonomous driving. In the foreseeable future, it will be unfeasible to forgo Bluetooth, WLAN, or cellular in the vehicle *(Fig. 1)*.

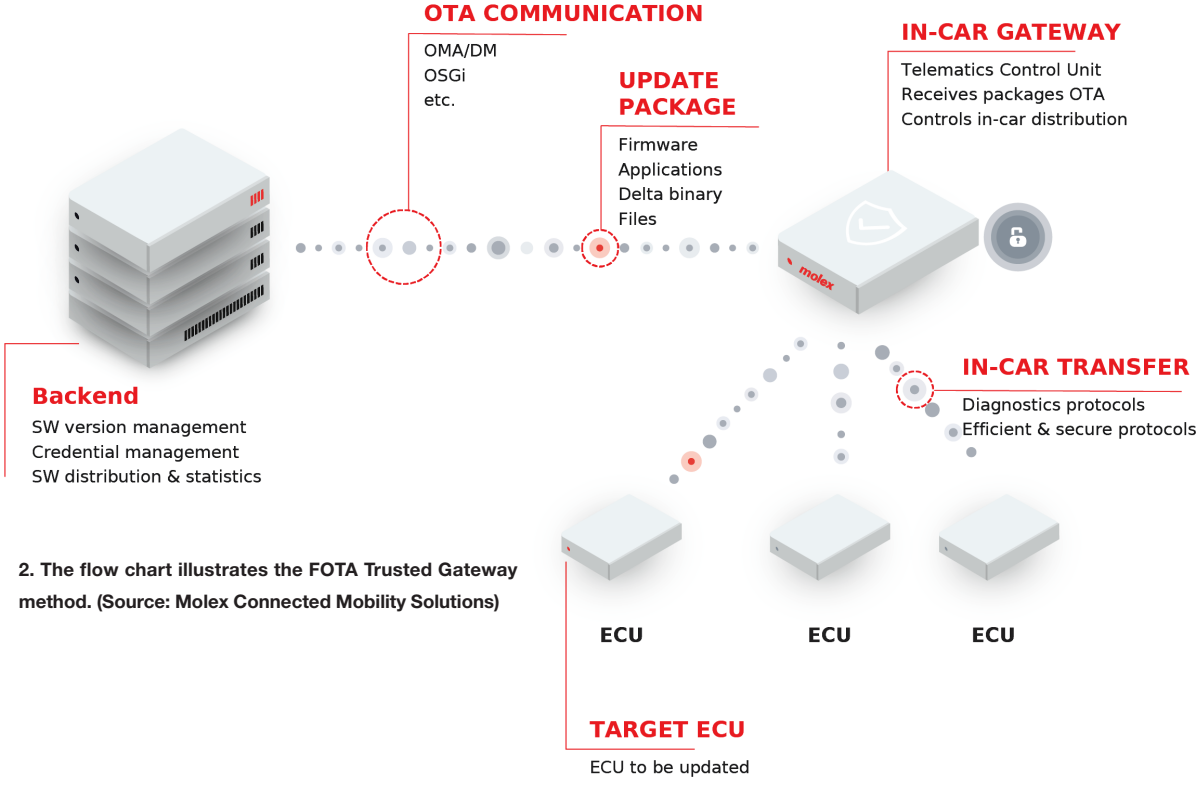
The dynamic nature of connectivity makes the traditional "call back" approach for addressing security issues in automotive repair shops inadequate to proactively safeguard vehicles against digital assailants. Widespread recall campaigns can be tremendously costly and damaging to the reputation of the manufacturer and brand. The race against car hackers cannot be won using outdated defenses. Providing a patch to all potentially jeopardized vehicles might extend months—or even years. In the meantime, hackers intent on creating mischief—or wreaking havoc—seldom rest.

Any delay to ward off potential danger due to a safety or security gap is unacceptable. Manipulated vehicles can pose enormous risks to drivers as well as their environment. Moreover, a hacker who successfully breaches existing security can potentially identify further weaknesses in the vehicle software, so the latest patch may already be obsolete at the time of its installation.

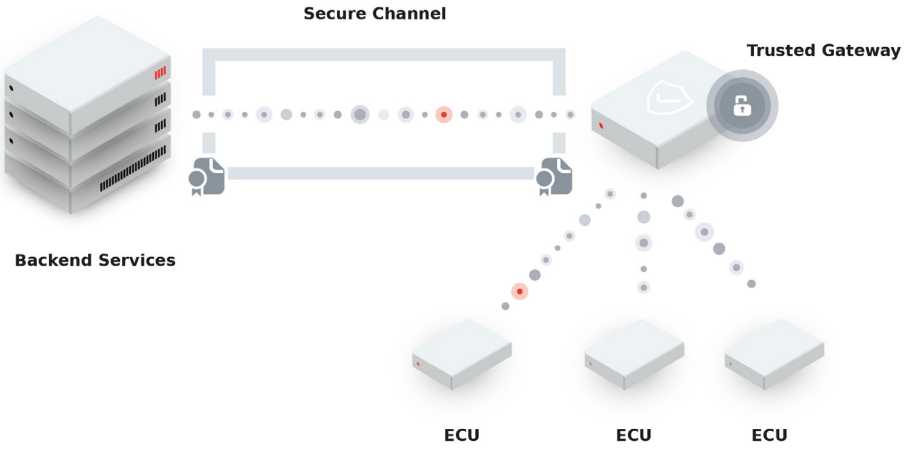
The mobile-device industry provides numerous insights into alternatives to repair recalls. Suppliers of apps and smartphone operating systems must constantly deliver up-to-date versions of their products directly to end-user devices. In some cases, a small patch may be designed to address a specific weak spot, or an update might entail the launch of an entirely new software or version of the operating system features that also introduces stronger security patches.

Mobile device software and firmware updates are delivered "over the air" (OTA), typically via air interfaces. As soon as the updates are transmitted to the device, they're 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 for swift and continuous remedy of weak spots with appropriate patches, while at the same time integrating new functions and modernizing cryptographic methods to secure, for example, the control units.

A gateway method can be employed to make sure that a large number of control units are updated by FOTA. Between the backend 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 higher-performing 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 *(Fig. 2)*.



2. The flow chart illustrates the FOTA Trusted Gateway method. (Source: Molex Connected Mobility Solutions)



3. Shown is the FOTA process chain and the functional units involved. (Source: Molex Connected Mobility Solutions)

A Paradigm Change

Apart from the possibility of closing security gaps by FOTA, many other technical measures are necessary on the device side. This includes 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 aren't the rule. However, by now, they should be a mandatory part of the requirements manufacturers demand of their suppliers. In this endeavor, possible scenarios of attack on 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 be guaranteed only if the OEM, the supplier of the back-end solution, and the control unit manufacturers cooperate from an early stage of development and onward. 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.

This approach requires rejecting the traditional black-box development of control units and instead embracing a more holistic approach to security. 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 of specifications related to all 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. In particular, penetration tests make it possible to pinpoint 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 that development of countermeasures are needed to seal off critical weak spots.

Technical Challenges

Taking a look at the FOTA process chain and the functional units involved provides important insights into the complexity and the advanced technical requirements. Within this ecosystem, security has the highest priority. There must be assurances that the FOTA process 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's 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 a 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 *(Fig. 3)*.

Development interfaces such as UART, USB, or JTAG must either be deactivated in the serial product or safeguarded by cryptographical procedures 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 significantly influence the size of the data packets.

The FOTA process must be very robust and fault tolerant to prevent the installation of incompatible, corrupt, or inconsistent software resulting in impaired functionality. The rapid identification of errors through integrity inspections and the supervision of the communication channels are both critically important. When there's an error, appropriate responses are required, e.g., by way of rollback actions that reestablish 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), though, is better equipped for this task than other units. The head unit, for instance, is an integral part of many vehicles, too, and 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, Wi-Fi, or NFC, with a multitude of requirements. This fundamental openness to the outside world impedes effective safeguarding against manipulation.

Moreover, the fact that it's installed directly into the dashboard precludes defining the head unit as the central FOTA gateway. After all, hackers might have rather easy physical access as well.

The physical location of the TCU, however, lies deeper within the vehicle and would be difficult to access from the vehicle's cabin. Overall, it has fewer connections, and these can be deactivated when the need arises.

Also, many other security-critical functions are already processed 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 backend, are a matter of course. The TCU has already become a well-established component of the security topology used by the manufacturers.

This is an advantage because we need holistic solutions if vehicles are to be secured. The backend, 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, too.

Projects where the TCU is at the center of a FOTA architecture don't have 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 experienced in designing secure processes.

Further Added Value in FOTA

Security concerns aren't 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 software-related problems show up in the vehicle. Many problems will be solvable 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.

In establishing these new business models and customer relations, FOTA can 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 a certain extra fee included an autopilot function. In this way, many Teslas have continued to develop into (partially) autonomous vehicles.

For OEMs, this setting opens an extraordinary new perspective. Today, it's common for the value of a new car to decrease as soon as it leaves the dealership. As time goes on, the value keeps diminishing. In the future, a vehicle might not necessarily lose value due to new functionalities. Rather, it might actually increase in value or at least retain more of its value due to future firmware and software enhancements. That's a selling point for automakers and an added value for prospective car buyers.

In these ways, FOTA provides a higher level of commitment that extends beyond safety and security. The wireless update procedure isn't just significant because it meets basic prerequisites of effective security for connected cars. An innovative OEM can create added value in the vehicle, boost customer loyalty, and keep revitalizing customer relations long after the original sale.

Standardization of FOTA is Essential

Molex understands the critical need to ensure that security and safety are top priorities as these changes occur. Molex has joined likeminded companies to form an alliance known as eSync to address the need for developing and promoting the technology required for automotive OTA and in-vehicle networks.

This industry-wide initiative is working to reduce the cost of software and firmware updates, as well as the number of recalls, and improve data services for the connected car. The commitment to address a lack of standardization by promoting a secure and open path for end-to-end OTA vehicle data transmission helps OEMs create advances needed to further drive the industry.