print | close

4 Layers of Automotive Security

Electronic Design

Andy Birnie Timo Van Roermund

Thu, 2016-08-25 12:51

Vehicles are rapidly evolving, shedding older technologies for new with the hopes of creating a safer, more efficient standard. Many previously mechanical systems are being replaced with electrical systems, leading to highly computerized vehicles. Connectivity is also being introduced to help connect vehicles with the world around them, opening the connected car to a multitude of security problems.

4-Layer Security Framework

To properly prepare vehicles for their connected future, secure vehicle architecture must follow four layers of security *(see figure)* that together provide the right level of protection:

• Secure interfaces that connect the vehicle to the external world.

• Secure gateways that provide domain isolation.

• Secure networks that provide secure communication between control units (ECUs).

• Secure processing units that implement all of the features of the connected car.

Each layer provides a unique form of protection while adding to the defenses of the system as a whole. Let's take a closer look at these four layers:

Layer 1: Secure Interface

The common networks in vehicles today are completely unprotected. If a hacker gains access to the telematics control unit (TCU), he or she can then send spoofed CAN messages and gain control of safety critical items, like brakes.

Related

Musings from FTF 2015

Securing the 5G Network

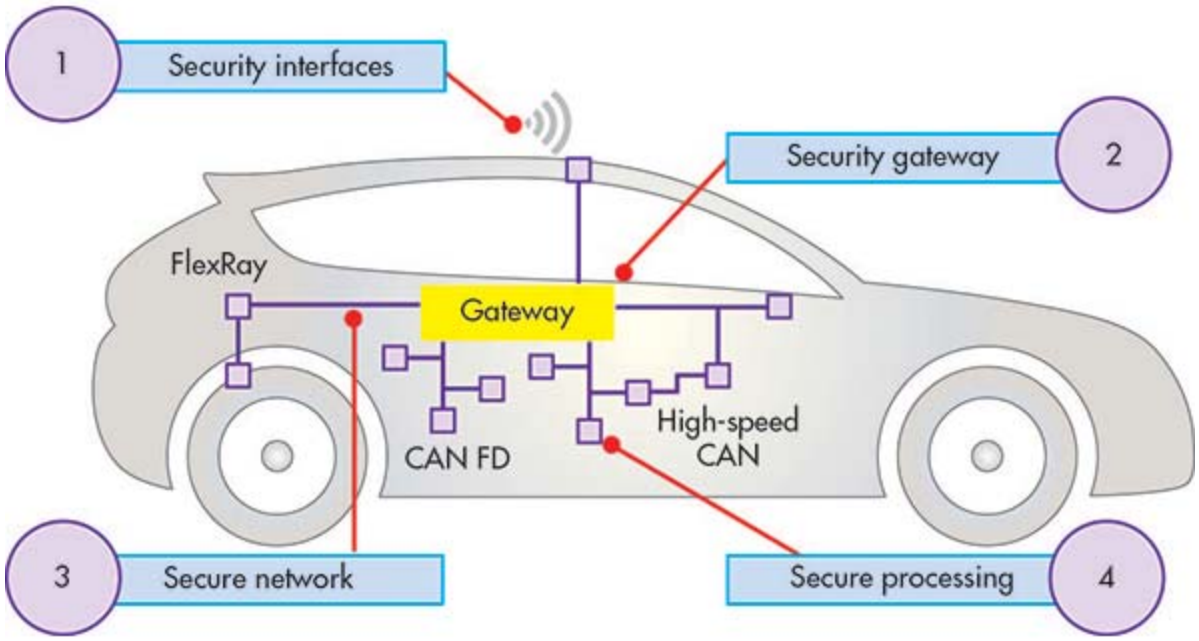
The Automotive Supercomputer

The first layer of protection adds security to the TCU by attaching a "secure element" for maximum security. Secure elements are dedicated security microcontrollers with high-performance cryptographic accelerators and proven advanced physical and electrical attack resistance—commonly used in ePassports, bank cards, and phones—that can be used to establish an end-to-end secure channel to the external world, also acting as ultra-secure vaults for keys and certificates.

ɣer 2: Secure Gateway

As we saw with last year's Jeep hack, once hackers obtain access to a network, they can send messages anywhere. This is where layer 2, the secure gateway, plays its part. A central gateway ECU separates the TCU and on-board diagnostics (OBD) from the network and breaks up the vehicle network into functional domains, with the gateway firewall deciding what nodes can legitimately communicate with other nodes.

In the Tesla Model S hack of 2015, the protection offered by the gateway was highlighted as a key security feature for modern vehicles. In the Jeep hack, hackers could switch off brakes remotely due to the lack of a gateway. In the Tesla hack, the worst they could do was sound the horn!



Apart from isolation, the most important function of the secure gateway is the firewall that separates the external interfaces from the safety-critical inner vehicle network. The gateway engine is a contextually aware routing function that determines, by a number of increasingly sophisticated checks, which messages are currently legitimate, and will pass through the gateway onto the destination.

Layer 3: Secure Network

With the network now split into domains, the attack surface of the architecture is significantly reduced, but the sub-domains are still vulnerable to attack. Layer 3 protects the sub-domains through the use of a secure network built of four safeguards:

1. *Message authentication scheme:* Each message is extended with a cryptographic code to guarantee an authentic sender and also that it was received unaltered.

2. *Encryption:* Data and identity theft can be avoided by encrypting the messages that are exchanged between different ECUs inside the vehicle.

3. *Intrusion detection:* Pattern recognition and rules checking to detect anomalies in the network traffic and to block malicious packets before they can even reach the microcontroller.

4. *ECU-level validation:* The authenticity of ECUs in the network can be verified regularly.

ɣer 4: Secure Processing

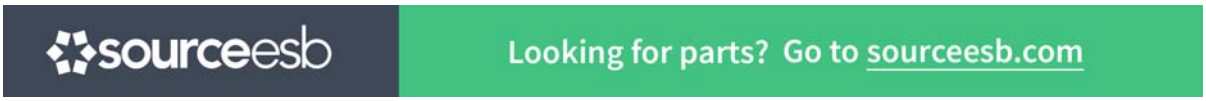
To tie it all together, we need to ensure the software running on the processor is genuine and trusted. To achieve that, modern microcontrollers feature secure boot and real-time integrity checking schemes to guarantee the code image is authentic, trusted, and unaltered. Mechanisms for controlled lockdown of the MCU and ECU through manufacturing are employed to lock out debug and serial download features, which would be invaluable to hackers.

On top of that, a secure software upgrade mechanism is needed. Modern vehicles average around 40 microcontrollers and millions of lines of code, creating massive software complexity. Such complex systems can't be perfect and vulnerabilities will be found after the vehicle hits the road.

When a bug or security vulnerability is detected, OEMs need the ability to quickly, seamlessly, and securely update the vehicle software, preferably without the need to visit the garage. The ability to perform over-the-air (OTA) software updates for every ECU in the vehicle is now demanded, and justified by the number and cost of vehicle recalls in the last few years.

Conclusion

We're in a new era of vehicle complexity and connectivity, and with that, a new era of ingenuity and resourcefulness for car hackers. However, the security of the vehicle electrical architecture is vital to ensure the safety of the vehicle occupants, so we need to respond to this threat. The 4-layer security framework provides a holistic approach for securing the complete vehicle architecture.



Source URL: http://electronicdesign.com/automotive/4-layers-automotive-security