Hardware-based Cybersecurity for Next-Generation Vehicles

It is now ten years since the European research project Evita radically changed the nature of embedded cybersecurity for vehicles. On the whole, safety-critical electronic control units in today's vehicles come with chips featuring both a central processing unit and a dedicated trust anchor, mainly in the form of a hardware security module. Escrypt has analyzed whether this approach can survive the advent of new onboard E/E architectures with higher real-time requirements and the need for greater bandwidth.

© Marisha Peshkova | shutterstock.com | Escrypt

AUTHORS

Suraj Ramachandrappa, M. Sc.
is Product Manager for embedded security software at Escrypt in Bochum, a brand of Etas GmbH in Stuttgart (Germany).

Dipl.-Ing. (TU) Raimund Stampa
is Lead Product Manager for embedded security software at Escrypt in Bochum, a brand of Etas GmbH in Stuttgart (Germany).

Ten years ago, the consortium behind Evita (E-Safety Vehicle Intrusion Protected Applications) project, funded by the European Commission, developed a new IT security architecture for automotive endpoints, covering the following versions: Evita Full, Evita Medium, and Evita Light [1, 2]. Despite being interpreted and implemented in various ways, the fundamental approach of Evita has proven to be extremely effective in practice and remains sound to this day: A dedicated, programmable on-chip hardware block that physically encapsulates the data to be protected, drives the related cryptographic operations while isolating them from the actual application side of the chip, thereby creating a dedicated security domain, also referred to as a Hardware Security Module (HSM) or Hardware Trust Anchor (HTA). Any data exchanged via the Electronic Control Unit (ECU) chip must cross a host-to-HSM bridge connecting these two domains. Typically, this bridge comprises interrupt signals, special function registers, and mailboxes in the form of shared memory or a software emulation thereof – for example using Interprocess Communication (IPC), **FIGURE 1**.

THE DE FACTO STANDARD FOR AUTOMOTIVE MICROCONTROLLERS

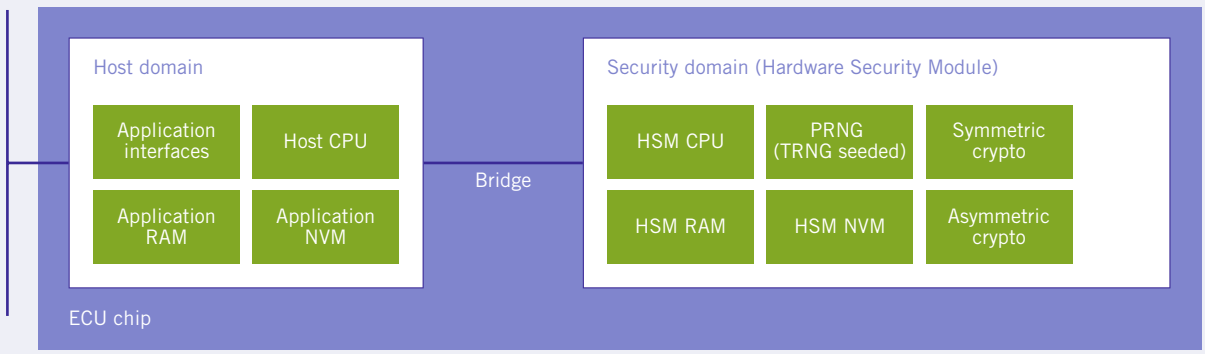
Today, this concept is well established and the de facto standard for onboard control units in automotive applications. It is used not only in onboard ECUs, but also in actuators and sensors, and for a host of applications, including onboard cameras, battery management, charging, airbags, brakes, and steering. The Evita security principle is now employed – chiefly in the form of a hardware security module – in almost all of the microcontrollers (MCUs) from chip manufacturers to the automotive industry as well as in Systems on a Chip (SoCs).

Yet after a decade, and in view of the challenges posed by future E/E vehicle architectures, the Evita architecture appears to be reaching its limits. The question is how best to adapt this tried-and-true approach, which is so vital for cybersecurity, and the future requirements of automotive MCUs.

SECURE ONBOARD COMMUNICATION REQUIRES EXTRA BANDWIDTH

Demand for Secure Onboard Communication (SecOC) continues to rise at a dramatic rate. Via external interfaces alone, today's vehicles communicate not only with diagnostic systems but also with charging stations, with cell phones – for example to lock/unlock and start the vehicle –, with other vehicles and traffic systems (vehicle-to-everything (V2X) communications), and with cloud systems for example to download newest software updates. In all of this, gateway modules act as communication hubs. At the same time, onboard internal communications are also on the increase. For example, the sensors required for autonomous driving need to collect, preprocess, and forward large volumes of data to domain and zone controllers. In addition, the introduction of a service-oriented proxy/skeleton architecture for onboard modules also generates additional network traffic.

All of this communication needs to be secured. On the sender side, Message Authentication Codes (MACs) are generated and added to the encrypted message. On the receiver side, a MAC is used to verify the authenticity of the message, which is then decrypted. This means that all the data has to cross a bridge between the application domain, located on the host core of the MCU, and the



	Full	Medium	Light
Independent CPU	✓	✓	✗
Host bridge	✓	✓	✓
PRNG (TRNG seeded)	✓	✓	✗
Symmetric cryptography (AES, ...)	✓	✓	✓
Asymmetric cryptography (ECC, RSA, SHA, ...)	✓	✗	✗

FIGURE 1 In the Evita architecture, the host and security domains are separated from one another on the hardware side (NVM: Non-volatile Memory; RAM: Random-access Memory; PRNG: Pseudo-random Number Generator; TRNG: True Random Number Generator) (© Escrypt)

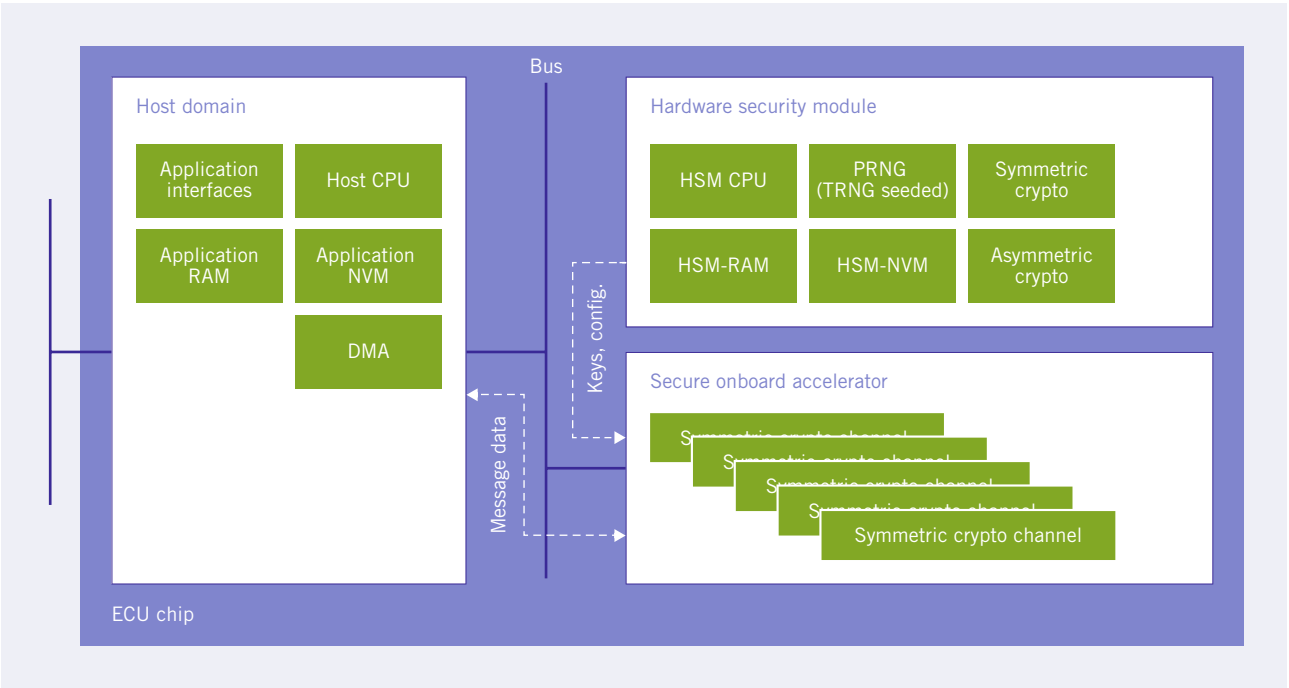


FIGURE 2 Next-generation automotive ECU chip: A performance-enhanced SecOC accelerator encrypts message traffic on the basis of key material provided by the HSM (© Escrypt)

security domain, which is the HSM core. This leads to a severe bottleneck. For this reason, today's high-end security software stacks are equipped with special mechanisms to ensure that the crypto hardware is assigned the greatest possible bandwidth, while interaction with the host Central Processing Unit (CPU) is kept to a minimum.

PERFORMANCE-ENHANCED CHIP ARCHITECTURE

Meanwhile, the advent of a new hardware concept has taken the next generation of automotive MCU architectures to another level. This involves adding a special performance-enhanced SecOC accelerator to the chip, alongside an HSM. Messages are then streamed through this accelerator block by using Direct Memory Access (DMA) functions linked to multiple, parallel, First-In, First-Out (FIFO) queues. Each channel applies symmetric cryptography such as AES-256 to the data. Meanwhile, the keys are derived from the classic hardware security module and injected into the SecOC accelerator unit. The transfer via an interconnect bus is secured by additional hardware mechanisms. Typically, this new hardware block is configurable but not programmable. In Evita terminology, this is equivalent to connecting an Evita Full unit to an Evita Light unit via a secure bus interface and then integrating them onto a single chip, **FIGURE 2**.

A side benefit of this modified architecture is that it substantially simplifies the implementation of safety requirements relating to communication. As such, safety-critical messages are processed securely and in isolation from other security applications, which for example allows secure booting, secure protocol execution via so-called Safe CMAC, i.e. by means of block Cipher-based Message Authentication Codes (CMACs) [3].

HYPERVISOR VIRTUALIZATION

Embedded cybersecurity in vehicles has to meet a whole range of rigorous requirements. For a start, it may well be that applications on the host side have been developed by a number of different suppliers working within an agile environment and independently to the actual hardware supplier. In this case, there needs to be a way of performing partial, dynamic Software-Over-The-Air (SOTA) updates without compromising other areas of the software. With platform concepts, it is possible to secure the same software functionalities – depending on the automobile manufacturer – with different sets of keys and certificates. If a hacker does manage to breach defenses and take control of an individual host application, it is vital that other applications continue to function securely. At the same time, different functions may also have different security levels and must therefore be isolated from one another. Nonetheless, all applications must still be able to simultaneously access the same hardware security module so as to benefit from its protection.

All of these scenarios can be realized by means of a virtual machine based on a hypervisor (HVR) that is supported by vendor hardware. Such hardware blocks are already standard on SoCs and are now being introduced – usually in a leaner form – in a new generation of automotive MCUs. Today's high-end security software stacks used for the HTA already support multicore applications. However, software mechanisms are only partially effective at isolating those applications from each other. Therefore, new MCU architectures have mechanisms to tag and identify security applications such as SecOC or sensitive data, so that these applications can then

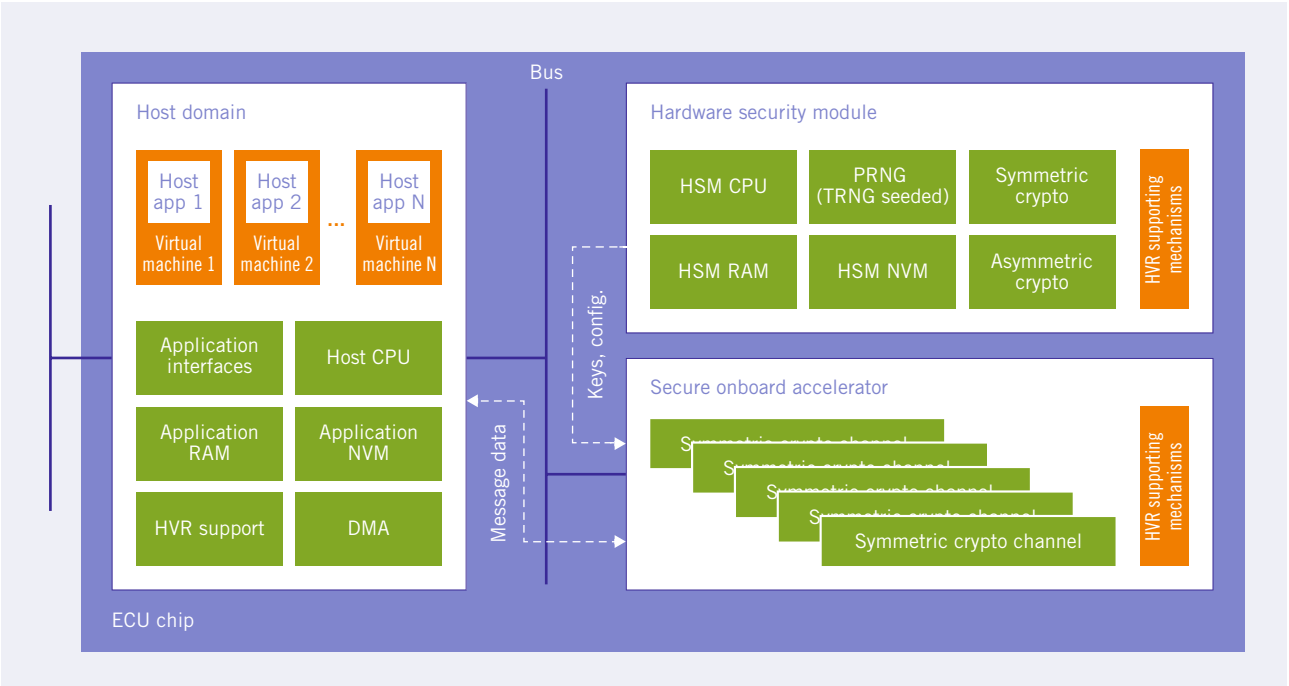


FIGURE 3 In the next generation of automotive MCUs, the use of virtual machines will make it possible to assign CPU resources to a number of securely isolated applications (© Escrypt)

be clearly assigned to a specific virtual machine. Conversely, this means that this data is not available to other virtual machines, making it possible to create individual security domains that are isolated from one another, **FIGURE 3**.

SECURITY FOR SOFTWARE-DEFINED VEHICLES

The advent of connected and increasingly software-defined mobility will pose new challenges for automotive cybersecurity. In response, the next generation of MCUs will boast enhanced hardware-security features in combination with an appropriately powerful security software stack for the HTA. In other words, hardware-based embedded cybersecurity – the core principle behind Evita – is set to retain its validity in the future. At the same time, the introduction of additional security hardware blocks and virtualization mechanisms will relieve bottlenecks that might otherwise result from increasing real-time response requirements and the need for greater communication bandwidth.

In turn, this will create new opportunities. Since the classic hardware security module no longer needs to provide SecOC functionality – which otherwise consumes a lot of resources – it can now perform a greater degree of other security tasks within the system. Moreover, greater memory availability will reduce the necessity for manufacturer-specific configurations.

In addition, the use of crypto hardware for post-quantum cryptography and Chinese crypto algorithms are set to grow in importance and will certainly play a role in hardware design of the future [4]. Similarly, the use of onboard Ethernet will boost demand for Ethernet-based security – key solutions being MACsec, IPsec and TLS. The shift toward highly connected, software-defined vehicles is gaining momentum, and automotive cybersecurity must move with this trend.

REFERENCES

[1] Fraunhofer Institute for Secure Information Technology (ed.): Evita – E-safety vehicle intrusion protected applications. Online: https://www.EVITA-project.org/, access: December 15, 2021

[2] Henniger, O.; et al.: Securing Vehicular On-Board IT Systems: The Evita Project. Online: https://www.EVITA-project.org/Publications/HRSW09.pdf, access: December 15, 2021

[3] Bierbaum, D.; Stampa, R.: Smart Synthesis of Cybersecurity and Functional Safety. In: ATZelectronics worldwide 6/2021, pp. 8-11

[4] Katsigianni, E.; Weigl, S.: Schutz vor Cyberattacken aus dem Quantencomputer: Die Post-Quantum-Challenge. In: Hanser automotive 6/2021, pp. 18 ff.