Hardwarebasierte Cybersicherheit für die nächste Fahrzeuggeneration

Vor zehn Jahren hat das europäische Forschungsprojekt Evita die eingebettete Cybersicherheit in Fahrzeugen neu konzipiert: Kritische Fahrzeugsteuergeräte sind heute in der Regel mit Chips bestückt, die neben dem Hauptprozessor einen dedizierten Security-Vertrauensanker mitbringen, meist in Gestalt eines Hardware-Security-Moduls. Escrypt hat analysiert, ob dieses Konzept im Zeitalter neuer E/E-Architekturen mit höheren Bandbreiten- und Echtzeitanforderungen weiterhin bestehen kann.

© Marisha Peshkova | shutterstock.com | Escrypt

AUTOREN

Suraj Ramachandrappa, M. Sc.
ist Produktmanager für eingebettete Security-Software bei Escrypt in Bochum, einer Marke der Etas GmbH in Stuttgart.

Dipl.-Ing. (TU) Raimund Stampa
ist leitender Produktmanager für eingebettete Security-Software bei Escrypt in Bochum, einer Marke der Etas GmbH in Stuttgart.

Vor zehn Jahren hat das Konsortium um das von der Europäischen Kommission geförderte Projekt Evita (E-Safety Vehicle Intrusion Protected Applications) eine IT-Sicherheitsarchitektur für automobile Endpunkte in den Varianten Evita Full, Evita Medium und Evita Light entwickelt [1, 2]. Obwohl in der Folge auf vielfältige Weise implementiert und interpretiert, ist der grundlegende Ansatz von Evita nach wie vor richtig und hat sich in der Praxis als überaus wirkungsvoll erwiesen: Ein dediziert programmierbarer On-Chip-Hardwareblock kapselt die schützenswerten Daten und die kryptografischen Operationen von der eigentlichen Anwendungsseite des Chips physikalisch ab und schafft so eine eigene Security-Domäne, auch bezeichnet als Hardware-Security-Modul (HSM) oder Hardwarevertrauensanker (Hardware Trust Anchor, HTA). Alle Daten, die über den Chip des elektronischen Steuergeräts (Electronic Control Unit, ECU) ausgetauscht werden, müssen dort die Brücke zwischen den beiden Bereichen, die sogenannte Host-to-HSM-Bridge, passieren. Diese Bücke besteht typischerweise aus Interrupt-Signalen, speziellen Funktionsregistern und Mailboxen in Form von gemeinsam genutztem Speicher (Shared Memory) beziehungsweise deren Softwareemulation, zum Beispiel unter Verwendung von Prinzipien der Interprozesskommunikation (Inter-Process Communication, IPC), **BILD 1**.

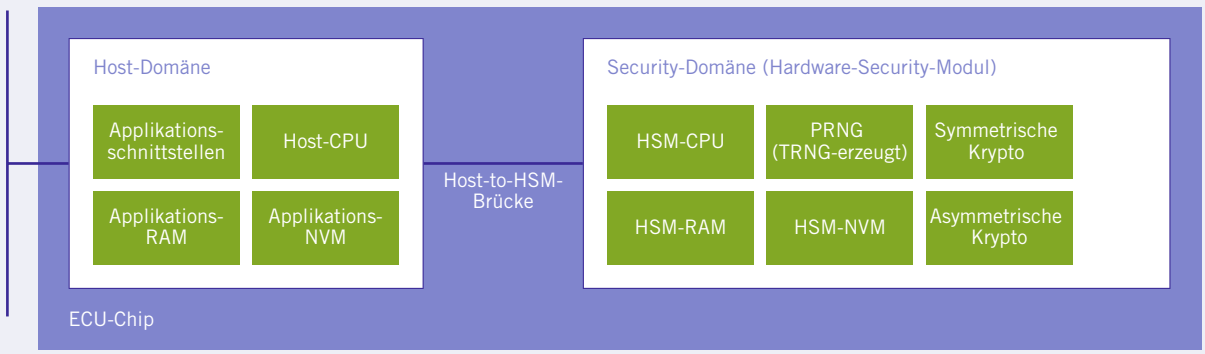
DE-FACTO-STANDARD FÜR AUTOMOBIL-MIKROCONTROLLER

Heute ist dieses Konzept weitgehend etabliert und bildet den De-facto-Standard für Onboard-Steuereinheiten im Automobilbereich. Es findet Verwendung auf ECUs, aber auch auf Aktoren und Sensoren und für alle Arten von Anwendungen wie Kameras, beim Batterie- und Lademanagement, bei Airbags, der Bremse oder der Lenkung. Das Evita-Security-Prinzip ist heute, zumeist in Gestalt von HSM, auf fast allen Mikrocontrollern (Micro Controller Units, MCUs) von Chip-Herstellern für die Automobilindustrie sowie in System-on-Chips (SoCs) implementiert.

Allerdings scheint die Evita-Architektur nach einem Jahrzehnt angesichts der Herausforderungen künftiger E/E-Architekturen an ihre Grenzen zu stoßen. Es stellt sich die Frage, wie sich der für die Cybersicherheit so wichtige und bewährte Evita-Ansatz mit den künftigen Leistungsanforderungen an Automobil-MCUs verbinden lässt.

ENGPASS FÜR DIE SICHERE ONBOARD-KOMMUNIKATION

Der Bedarf an sicheren Möglichkeiten für die Onboard-Kommunikation (Secure Onboard Communication, SecOC) nimmt drastisch zu. Nimmt man allein die externen Schnittstellen, so kommuniziert das moderne Fahrzeug nicht nur mit Diagnosesystemen, sondern auch mit der Ladestation, dem Mobiltelefon – beispielsweise zum Ver- und Entriegeln oder zum Starten des Fahrzeugs –, anderen Fahrzeugen und Verkehrssystemen (Vehicle-to-Everything (V2X)-Kommunikation) oder der Cloud, etwa zum Herunterladen von Software-Updates. Gateway-Module fungieren dabei als Kommunikationsdrehscheibe. Zugleich nimmt auch die interne Kommunikation zu: Sensoren für das autonome Fahren müssen große Datenmengen sammeln, vorverarbeiten und an die Domänen- und Zonencontroller weiter-



	Full	Medium	Light
Unabhängige CPU	✓	✓	✗
Host-Brücke	✓	✓	✓
PRNG (TRNG-erzeugt)	✓	✓	✗
Symmetrische Kryptografie (AES …)	✓	✓	✓
Asymmetrische Kryptografie (ECC, RSA, SHA …)	✓	✗	✗

BILD 1 Evita-Architektur – Host- und Security-Domäne sind hardwareseitig voneinander getrennt (CPU (Central Processing Unit): Prozessor; NVM (Non-Volatile Memory): nichtflüchtiger Speicher; RAM (Random-Access Memory): schnellflüchtiger Speicher; PRNG (Pseudo Random Number Generator): Pseudozufallszahlengenerator); TRNG (True Random Number Generator): Hardware-Zufallszahlengenerator) (© Escrypt)

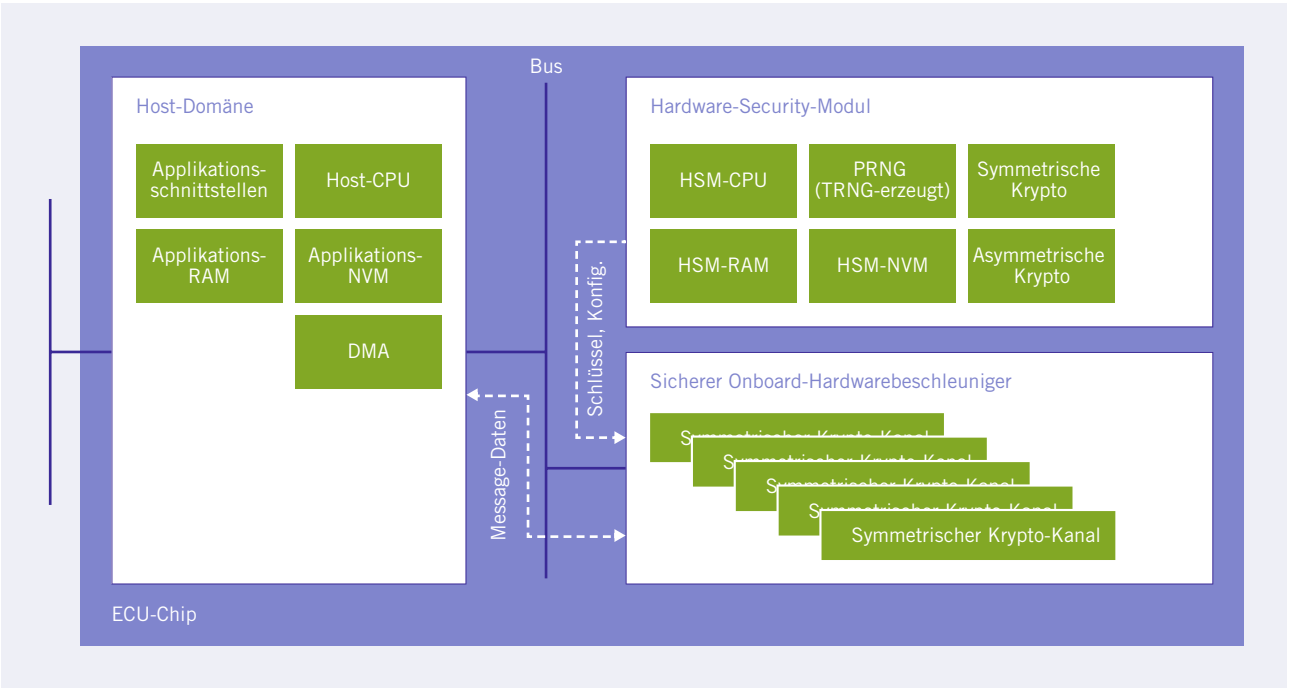


BILD 2 Automobil-ECU-Chip der nächsten Generation – ein leistungsoptimierter SecOC-Beschleuniger übernimmt die kryptografische Verschlüsselung der Nachrichten, während das HSM das Schlüsselmaterial bereitstellt (© Escrypt)

leiten. Die Einführung der serviceorientierten Proxy-Skeleton-Architektur zwischen den Onboard-Modulen führt zu zusätzlichem Netzwerkverkehr.

Diese gesamte Kommunikation gilt es abzusichern. Auf Absenderseite werden Nachrichtenauthentifizierungscodes (Message Authentification Codes, MACs) erzeugt und der verschlüsselten Nachricht hinzugefügt. Auf Empfängerseite wird anhand des MACs dann die Authentizität überprüft, und die Nachricht wird entschlüsselt. Das bedeutet, dass alle Daten die Brücke zwischen dem Anwendungsbereich auf dem Host-Core der MCU und der Security-Domäne, dem HSM-Core, passieren müssen. Und das wiederum führt zu einem erheblichen Engpass. High-End-Security-Softwarestacks verfügen daher heute über spezielle Mechanismen, um die Krypto-Hardware mit größtmöglicher Bandbreite zu nutzen und gleichzeitig die Interaktion mit dem Host-Prozessor auf ein Minimum zu reduzieren.

LEISTUNGSOPTIMIERTE CHIP-ARCHITEKTUR

Die nächste Generation von MCU-Architekturen für den Automobilbereich indes schwingt sich hier dank eines neuen Hardwarekonzepts in neue Sphären auf. Dafür ist ein spezieller leistungsoptimierter SecOC-Beschleuniger zusätzlich zum HSM auf dem Chip implementiert. Nachrichten werden durch diesen Beschleunigerblock geleitet, indem Direct-Memory-Access(DMA)-Funktionen mit mehreren parallelen First-in-First-out-Warteschlangen (FIFO-Queues) verbunden werden. Jeder Kanal verarbeitet symmetrische Kryptografie wie AES-256 auf den Daten, während die Schlüssel vom klassischen HSM abgeleitet und in die SecOC-Beschleunigereinheit injiziert werden. Die Übertragung über den Interconnect-Bus wird durch zusätzliche Hardwaremechanismen gesichert. Typischerweise ist dieser neue Hardwareblock konfigurierbar, aber nicht programmierbar. In der Evita-Terminologie hieße das, dass eine Evita-Full-Einheit mit einer Evita Light-Einheit, verbunden über eine gesicherte Bus-Schnittstelle, kombiniert und in einen einzigen Chip integriert wird, **BILD 2**.

Positiver Nebeneffekt einer derart veränderten Architektur ist die wesentlich einfachere Umsetzung von Safety-Anforderungen rund um die Kommunikation: Die Verarbeitung der Safety-kritischen Nachrichten erfolgt abgesichert und isoliert von anderen Security-Anwendungen und erlaubt so unter anderem sicheres Booten und sichere Protokollierung per sogenanntem Safe CMAC, also mittels blockchiffrebasierter Nachrichtenauthentifizierungscodes (Cipher-based Message Authentication Code, CMAC) [3].

VIRTUALISIERUNG PER HYPERVISOR

Die Ansprüche an eingebettete Cybersicherheit im Fahrzeug sind vielfältig und hoch: Anwendungen auf der Host-Seite können von verschiedenen Zulieferern in einem agilen Ansatz und unabhängig vom Lieferanten der Hardware mitentwickelt werden. Das heißt, partielle dynamische Software-Updates Over-the-Air (SOTA) müssen möglich sein, ohne andere Teile der Software zu beeinträchtigen. Bei Plattformkonzepten kann dieselbe Softwarefunktion – abhängig vom Automobilhersteller – mit unterschiedlichen Sets von Schlüsseln und Zertifikaten gesichert werden. Denn wenn es einem Angreifer gelingt, in eine einzelne Host-Anwendung einzudringen und ihre Kontrolle zu übernehmen, sollen andere Anwendungen weiterhin abgesichert funktionieren. Zudem können verschiedene Funktionen unterschiedliche Sicherheitsstufen haben und müssen daher voneinander isoliert werden.

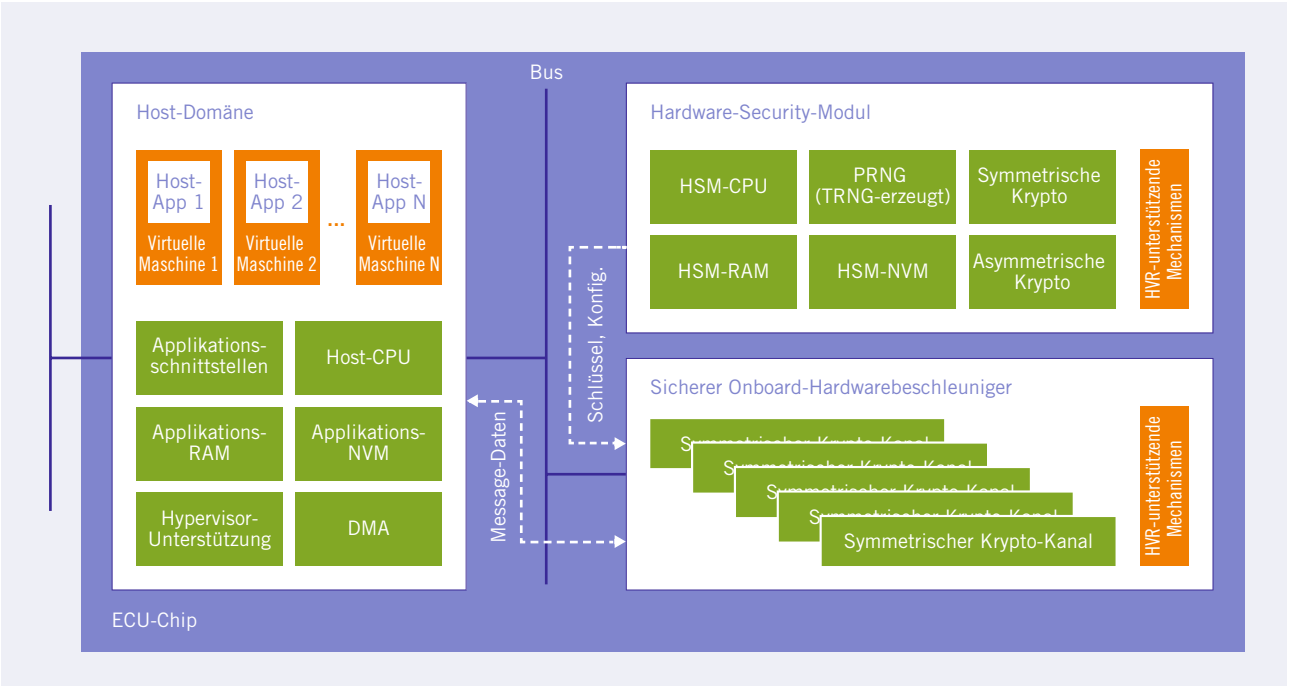


BILD 3 Die nächste Generation der MCUs für Automobilanwendungen ermöglicht es, CPU-Ressourcen durch Virtualisierung mehreren sicher getrennten Anwendungen zuzuordnen (© Escrypt)

Gleichwohl müssen alle Anwendungen für die nötigen Security-Operationen zeitgleich auf dasselbe HSM zugreifen können.

Realisieren lassen sich all diese Szenarien durch Virtualisierungskonzepte auf Basis von herstellerseitig hardwareunterstützten sogenannten Hypervisoren (HVRs). Eine solche Hardwareunterstützung ist bereits Standard auf SoCs und wird nun auch – meist in abgespeckter Form – in einer neuen Generation von MCUs für Fahrzeuge eingeführt. Denn bestehende High-End-Security-Softwarestacks für den HTA unterstützen zwar bereits Multicore-Anwendungen. Die Isolation der Applikationen voneinander kann aber per Softwaremechanismen nur in Grenzen realisiert werden. Neue MCU-Architekturen implementieren daher Mechanismen, die Security-Anwendungen wie SecOC oder schützenswerte Daten so kennzeichnen und identifizieren, dass sie eindeutig einer bestimmten virtuellen Maschine zugeordnet werden können. Umgekehrt bedeutet dies, dass diese Daten den anderen virtuellen Maschinen nicht zur Verfügung stehen und somit einzelne voneinander isolierte Sicherheitsdomänen geschaffen werden können, **BILD 3**.

SECURITY FÜR SOFTWARE-DEFINIERTE FAHRZEUGE

Die verbesserten Hardware-Security-Funktionen der nächsten MCU-Generation in Kombination mit einem entsprechend leistungsstarken Security-Softwarestack für den HTA werden die Cybersecurity-Herausforderungen der vernetzten, zunehmend softwaredefinierten Mobilität der Zukunft meistern. Während das Evita-Grundprinzip der hardwarebasierten eingebetteten Cybersicherheit seine Gültigkeit weiterhin behält, werden steigende Bandbreiten- und Echtzeitanforderungen durch zusätzliche Security-Hardwareblöcke und Virtualisierungsmechanismen aufgefangen und drohende Engpässe vermieden.

Damit eröffnen sich neue Möglichkeiten: Da das klassische HSM von der leistungsfordernden SecOC-Funktion befreit wird, kann es nun andere Security-Aufgaben im System übernehmen. Zugleich ließe sich durch die höhere Speicherverfügbarkeit der Bedarf an herstellerspezifischen Konfigurationen verringern.

Darüber hinaus wird Krypto-Hardware zur Unterstützung der Post-Quanten-Kryptografie und zur Unterstützung chinesischer Krypto-Algorithmen an Bedeutung gewinnen und muss bei der Auslegung der Hardware von morgen berücksichtigt werden [4]. Und der Einsatz von Ethernet im Fahrzeug wird die Nachfrage nach ethernetbasierter Sicherheit – Stichworte sind hier MACsec, IPsec und TLS – erhöhen. Die Entwicklung hin zum softwaredefinierten, hochgradig vernetzten Fahrzeug gewinnt also an Geschwindigkeit, und die Automotive Cybersecurity muss hier mitgehen.

LITERATURHINWEISE

[1] Fraunhofer-Institut für Sichere Informationstechnologie (Hrsg.): Evita – E-safety vehicle intrusion protected applications. Online: https://www.EVITA-project.org/, aufgerufen: 15. Dezember 2021
[2] Henniger, O. et al.: Securing Vehicular On-Board IT Systems: The Evita Project. Online: https://www.EVITA-project.org/Publications/HRSW09.pdf, aufgerufen: 15. Dezember 2021
[3] Bierbaum, D.; Stampa, R.: Smarte Synthese aus Cybersecurity und Funktionssicherheit. In: ATZelektronik 16 (2021), Nr. 6, S. 16-20
[4] Katsigianni, E.; Weigl, S.: Schutz vor Cyberattacken aus dem Quantencomputer: Die Post-Quantum-Challenge. In: Hanser automotive 20 (2021), Nr. 6, ab S.18