Schutz vor unbefugtem Zugriff

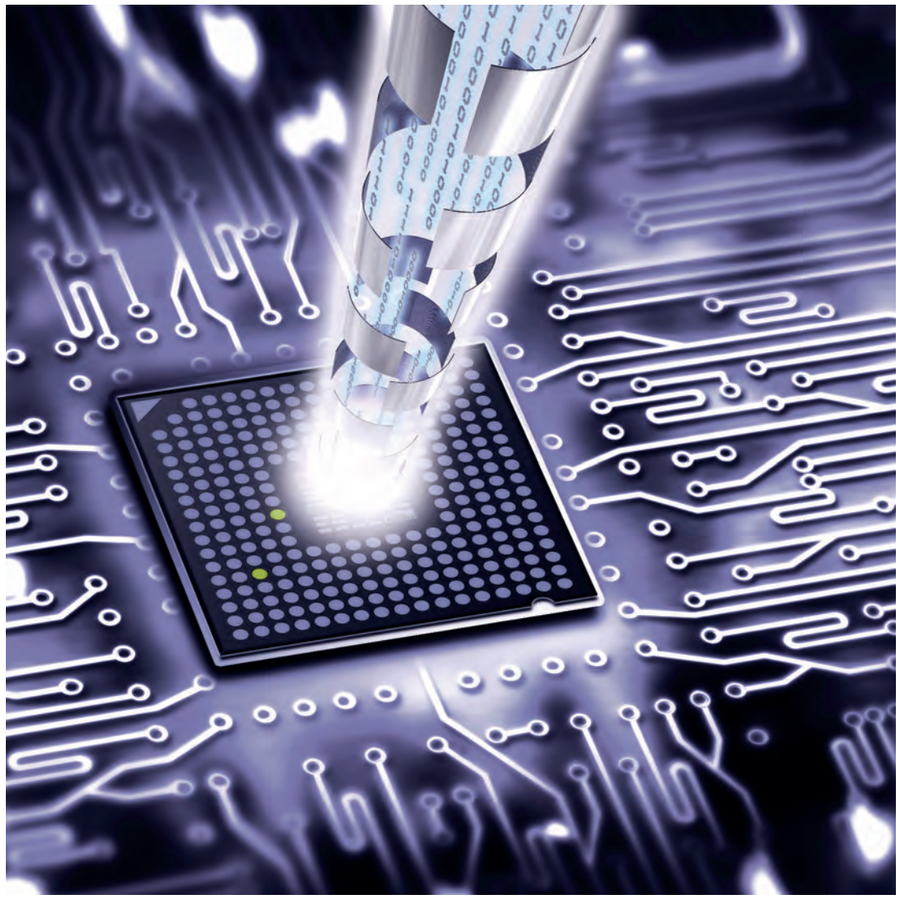
Intelligentes Miteinander von Soft- und Hardware schirmt Steuergeräte ab

Vernetzte Fahrzeugsysteme brauchen Schutz vor unbefugten Zugriffen. Hardware Security Modules (HSMs) bieten ihn, waren aber bisher nicht für den Einsatz im Automobil geeignet. Das Bosch HSM und seine Implementierungen verschiedener Halbleiterhersteller ändern das. Pünktlich zum Markthochlauf hat ESCRYPT mit CycurHSM eine passende Firmware auf den Markt gebracht. Mit ihr wird das HSM zum Sicherheitsdienstleister für Fahrzeugsteuergeräte.

AUTOREN

Christopher Pohl ist Senior Security Engineer bei der **ESCRYPT GmbH** in Bochum.

Dr. Frederic Stumpf leitet die **ESCRYPT-Niederlassung** in Stuttgart.



Ein Seitenfenster ist eingeschlagen. Airbags und Navi fehlen. Extrem ärgerlich. Aber zumindest erkennbar. Dagegen sind unbefugte Eingriffe in die Fahrzeug-IT eine unsichtbare Bedrohung, deren Risikopotential durch die zunehmende Vernetzung von Fahrzeugen und ihrer Steuergeräte (Electronic Control Units, ECUs) wächst.

Abwehrstrategien gegen Hackerangriffe, Virenkontamination oder unbefugte Uploads müssen her. Bosch hat das vor einigen Jahren erkannt und Hardware Security Modules (HSM) als geeignete Schutztechnologie identifiziert. Solche Module haben einen eigenen Prozessorkern, eigene RAM-, ROM- und Flash-Speicher sowie spezifische Sicherheits-Features. Allerdings waren verfügbare HSMs zu teuer, empfindlich und funktional eingeschränkt. Bosch entwickelte darum Spezifikationen für ein Automotive-taugliches HSM und teilte diese im Sinne zügiger Marktdurchdringung mit Halbleiterherstellern. Diese Strategie geht auf: Diverse Hersteller haben Derivate des Bosch HSMs realisiert, die nun auf den Markt drängen.

Standardisierter Software-Stack für Bosch HSM und deren Derivate

Seit Juli 2015 gibt es auch die passende Firmware: CycurHSM von ESCRYPT. Im intelligenten Zusammenspiel mit der Hardware schirmt sie Fahrzeugsysteme in jeder Betriebsphase gegen unbefugte Zugriffe ab – beim Booten, während des laufenden Betriebs und auch beim Aufspielen von Software-Updates oder -Upgrades. Hard- und Software arbeiten dabei Hand in Hand. Das Bosch HSM verfügt neben Prozessor und Speicher über einen True-Random-Number-Generator (TRNG), der echte Zufallszahlen generiert. Zudem erlaubt eine Beschleuniger-Hardware blitzschnelles Rechnen von kryptographischen Nachrichten-Authentifizierungscodes gemäß dem Advanced Encryption Standard (AES). Auf Basis dieser Hardware hat ESCRYPT die Funktionen „Secure Boot“, „Runtime Tuning Detection“ und „Secure Flashing“ in CycurHSM realisiert. Die Software setzt zudem auf RTA-OS von ETAS auf, das als Echtzeit-Betriebssystem für Automotive-Einsätze entwickelt wurde.

Volle Flexibilität bei der Hardware-Auswahl

Als Mitte 2013 die Überlegungen zu CycurHSM begannen, war es die Vision von ESCRYPT, einen standardisierten Software-Stack für das Bosch HSM und all seine Derivate zu entwickeln. Dieses Ziel ist erreicht: Die Standardisierung auf Software-Ebene erlaubt Kunden freie Auswahl der Controller – trotz aller Unterschiede der Hardware-Auslegung. Entsprechend der offenen Philosophie ist CycurHSM zudem nicht nur mit AUTOSAR kompatibel, sondern dank seiner CSAI-Schnittstelle (Client Server Architecture and Interface) auch für alle Anwendungen abseits dieses Standards.

Umfassender Schutz

CycurHSM ist in das modulare Produktportfolio von ESCRYPT eingebettet. So auch die „Secure Flashing“-Funktion der Firmware. Über diese müssen sich Absender von Updates oder Upgrades authentifizieren. Die dafür benötigten geheimen Schlüssel werden im Backend des Automobilherstellers oder eines spezialisierten Dienstleisters erzeugt und nur an vertrauenswürdige Partner weitergegeben. ESCRYPT bietet solches Key Management samt Abwicklung in Hochsicherheitsrechenzentren an. Oder wahlweise auch nur die Lizenzen für Software zum Erzeugen von solchen kryptographischen Schlüsseln. Gerade in Hinblick auf Car-to-X-Kommunikation und Over-the-Air-Updates benötigen Fahrzeuge Torwächterfunktionen wie das „Secure Flashing“. Kann ein Absender die digitalen Signaturen nicht liefern, verwehrt ihm das HSM den Datentransfer. Auf Verschlüsselungs-Know-how basiert auch die „Secure Boot“-Funktion in Cycur-HSM. Beim Booten kann diese anhand geheimer Schlüssel zweifelsfrei erkennen, ob Steuergerätesoftware noch authentisch ist.

Beim Hochfahren prüft dafür jede gestartete Komponente in der Boot-Chain der Steuergeräte die Integrität der jeweils nächsten. Das stellt sicher, dass Schadsoftware spätestens beim nächsten Start erkannt wird; selbst wenn sie über vertrauenswürdige Quellen an Bord gelangt – etwa ein Diagnosegerät in der Werkstatt. Da das HSM jede Veränderung aufzeichnet, bleibt Manipulation auch dann nachweisbar, wenn der Originalzustand der Steuergerätesoftware wiederhergestellt wird. So schafft CycurHSM quasi nebenbei Rechtssicherheit im Graubereich des Chiptunings.

Im laufenden Betrieb überprüft die „Runtime Tuning Detection“ von CycurHSM zyklisch, ob die Steuergerätedaten noch authentisch sind. Diese Überprüfung anhand symmetrischer AES-Signaturen erfolgt

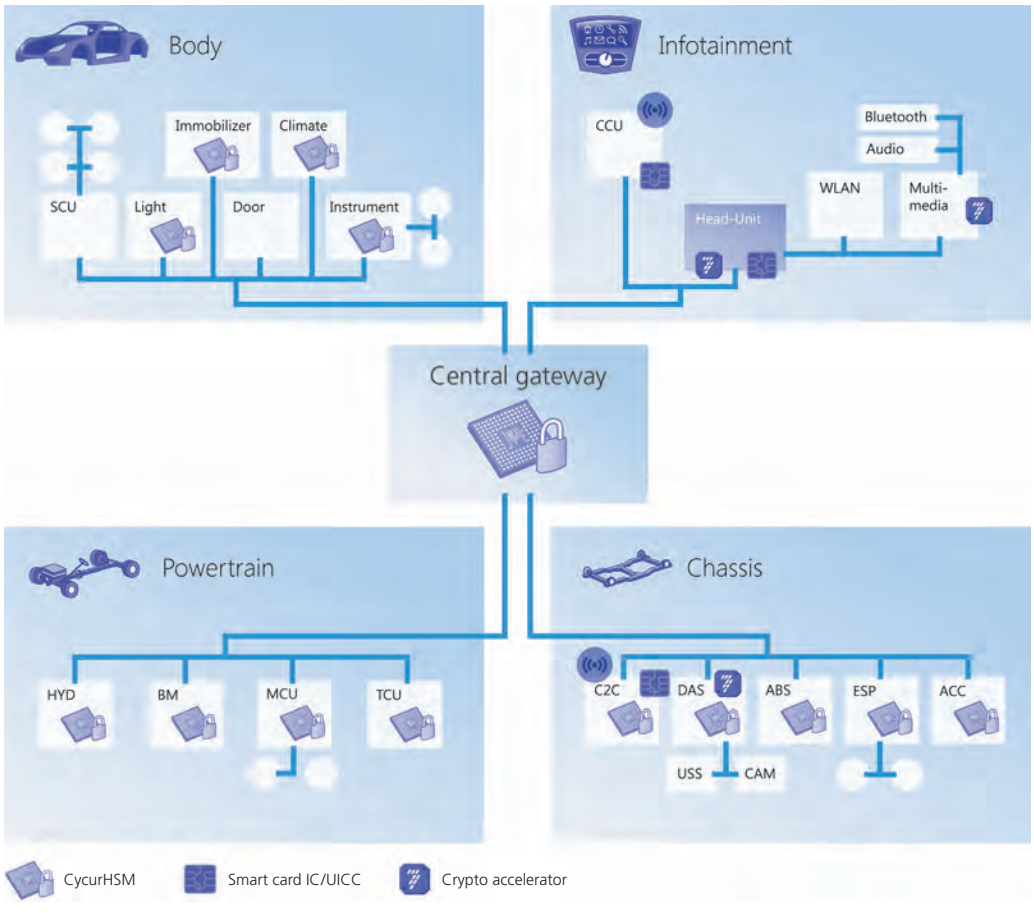
dank Beschleuniger-Hardware hocheffizient.

Mit „Secure On-Board Communication" bietet CycurHSM eine vierte Funktion, um den Datenaustausch von ECU zu ECU im Fahrzeug zu schützen. Sie schützt den Datenverkehr auf dem Fahrzeugbus gegen Angriffe, die z. B. Drahtlos-Schnittstellen im Fahrzeug als Einfallstor nutzen. Dafür versieht CycurHSM die Daten auf ihrem Weg von ECU zu ECU mit AES-basierten Nachrichten-Authentifizierungscodes und nimmt den beteiligten Steuergeräten das Generieren und Verifizieren der Codes ab. Es erledigt alle kryptographischen Rechenoperationen und das Verwahren der Schlüssel – agiert also wie ein integrierter Sicherheitsdienstleister der Steuergeräte.

Ausblick

ESCRYPT ist überzeugt, dass sich die HSM-Technologie im Laufe der nächsten zehn Jahre zur Standardausstattung von Neufahrzeugen entwickeln wird. Mit der standardisierten Software CycurHSM wird ein wichtiger Baustein geliefert, um der Technologie zum Durchbruch zu verhelfen. Im Zusammenspiel mit der HSM-Hardware schützt sie die sicherheitsrelevanten IT-Systeme im Fahrzeug vor unbefugtem Zugriff. Auch mit Blick auf die rasch voranschreitende Vernetzung ist das eine zukunftssichere Lösung.

Fahrzeug-Bordnetz in 202x.



SCU	Seat Control Unit
CCU	Communication Control Unit
HYD	Hybrid Drive
BM	Battery Management
MCU	Motor Control Unit
TCU	Transmission Control Unit
C2C	Car-to-Car Communication
DAS	Driver Assistance System
ABS	Anti-lock Braking System
ESP	Electronic Stability Program
ACC	Adaptive Cruise Control
USS	Ultrasonic Sensor
CAM	Camera
IC/UICC	Integrated Circuit/ Universal Integrated Circuit Card