© Escrypt

Immunsystem für das vernetzte Fahrzeug

Mit der Öffnung für die Außenwelt steigt auch die Gefahr von Cyber-Attacken und unbefugten Zugriffen auf Fahrzeugsysteme. Weil Angreifer ihre Strategien und Angriffspunkte häufig ändern, brauchen vernetzte Fahrzeuge ein lernendes Immunsystem. Es muss Angriffe auf das Bordnetz auch dann erkennen, wenn deren Methode bis dahin noch unbekannt sein sollte. Zudem sollte es seine Erfahrung zügig mit anderen Fahrzeugen im Feld teilen.

Für Autobesitzer beginnt der Lebenszyklus ihres Fahrzeugs mit dem Kauf und endet mit der Ausmusterung. Es ist die Phase, in der Automobilhersteller am wenigsten Zugriff auf die Fahrzeuge haben, aber dennoch höchste Sicherheitsanforderungen erfüllen müssen. Die Vernetzung von Fahrzeugen mit der Außenwelt erschwert diese Herausforderung zusehends. Denn es reicht nicht mehr, die funktionale Sicherheit (safety) der Systeme zu garantieren. Vielmehr rückt die IT-Sicherheit (automotive security) in den Fokus. Fahrzeugsysteme brauchen Schutz vor unbefugten Zugriffen und böswilligen Cyber-Attacken.

Prognosen zufolge werden schon in fünf Jahren über 380 Mio. Fahrzeuge vernetzt sein. Schnittstellen zu Smartphones und die Möglichkeit zur Car-to-x-Kommunikation schaffen vergrößerte Angriffsflächen. Zugleich nehmen Steuergeräte und deren Software dem Fahrer immer mehr

Nicht zur Verwendung in Intranet- und Internet-Angeboten sowie elektronischen Verteilern.
© 2017 Carl Hanser Verlag, München www.hanser-automotive.de

© Carl Hanser Verlag, München

© 2017 Carl Hanser Verlag, München www.hanser-automotive.de Nicht zur Verwendung in Intranet- und Internet-Angeboten sowie elektronischen Verteilern.

Verantwortung ab. Die Vision des automatisierten Fahrens wird sukzessive real. Diese neue, vernetzte Welt erfordert holistische Sicherheitsstrategien, in denen die funktionale Sicherheit und die Automotive Security untrennbar miteinander verknüpft sind.

Holistischer Schutz über den gesamten Lebenszyklus

Für sämtliche Abläufe in der Fahrzeugentwicklung und während der Produktion stehen heute erprobte Sicherheitskonzepte bereit. So folgt die Entwicklung der Embedded-Software für Steuergeräte standardisierten Prozessen, die auch deshalb ein Höchstmaß an Zuverlässigkeit gewährleisten, weil sie sicherheitsrelevante Schwachstellen frühzeitig aufdecken. Auch im Bereich Security wächst das Lösungsangebot stetig. Moderne Chip-Architekturen bieten Hardware-Security-Erweiterungen, durch die sicherheitsrelevante Systembereiche physikalisch gegen unbefugte Zugriffe abgesichert sind – darunter Hardware-Security-Module (HSM) oder Secure-Hardware-Extensions (SHE). Rund um diese Sicherheitskerne implementieren die Hersteller systematisch weitere Security-Funktionen. Seien es Secure-Boot-Funktionen, die mögliche Manipulationen an der Steuergeräte-Firmware erkennen können, geschützte Netzwerkübergänge (Gateways), die Onboard-Netzwerke mit gegebenenfalls verschiedenen Sicherheitsstufen zuverlässig voneinander trennen, oder seien es kryptographische Lösungen, mit denen Kommunikation innerhalb des Fahrzeugs, mit anderen Fahrzeugen sowie mit externer IT-Infrastruktur geschützt wird.

Hinzu kommen organisatorische Schutzmaßnahmen für Entwicklung und Produktion, die auf erprobten Security-Prozessen und -Funktionen basieren. Etwa zugangsbeschränkte Sicherheitsbereiche oder auf einige wenige Verantwortliche beschränkte Zugriffsrechte auf Krypto-Schlüssel und Freischaltcodes.

Schutz vor unbekannten Gefahren

Alle beschriebenen Schutzmaßnahmen senken die Wahrscheinlichkeit von zufälligen Fehlern und erhöhen den Aufwand für Angreifer, in die IT-Systeme von Fahrzeugen einzudringen und sie zu manipulieren. Doch bleibt die Frage, wie der Schutz der vernetzen Systeme zu gewährleisten ist, wenn das Fahrzeug in Kundenhand ist. Denn in dieser Kernphase des Lebenszyklus haben Hersteller nur bedingt Zugriff auf Fahrzeuge. Sie müssten diese also theoretisch für Angriffe wappnen, die über ein Jahrzehnt in der Zukunft liegen können. Ein Rückblick auf den Stand der Informationstechnologie vor einem Jahrzehnt genügt, um zu verstehen, dass ein solcher vorausschauender Schutz nicht vollständig möglich ist. Daraus folgt: Die Maßnahmen der IT-Sicherheit dürfen nicht enden, wenn das Fahrzeug die Fertigung verlässt. Vielmehr müssen die Systeme auch in Kundenhand dynamisch und zuverlässig gegen unbefugte Eingriffe und Cyber-Attacken abgeschirmt werden.

Aber wie? Während die Randbedingungen der funktionalen Sicherheit in den meisten Fällen auf Naturgesetzen und statistischen Vorhersagen beruhen, die im Betrieb weiter gelten, können sich die Annahmen und Randbedingungen der IT-Sicherheit jederzeit ändern. Denn Angreifer suchen syste- »

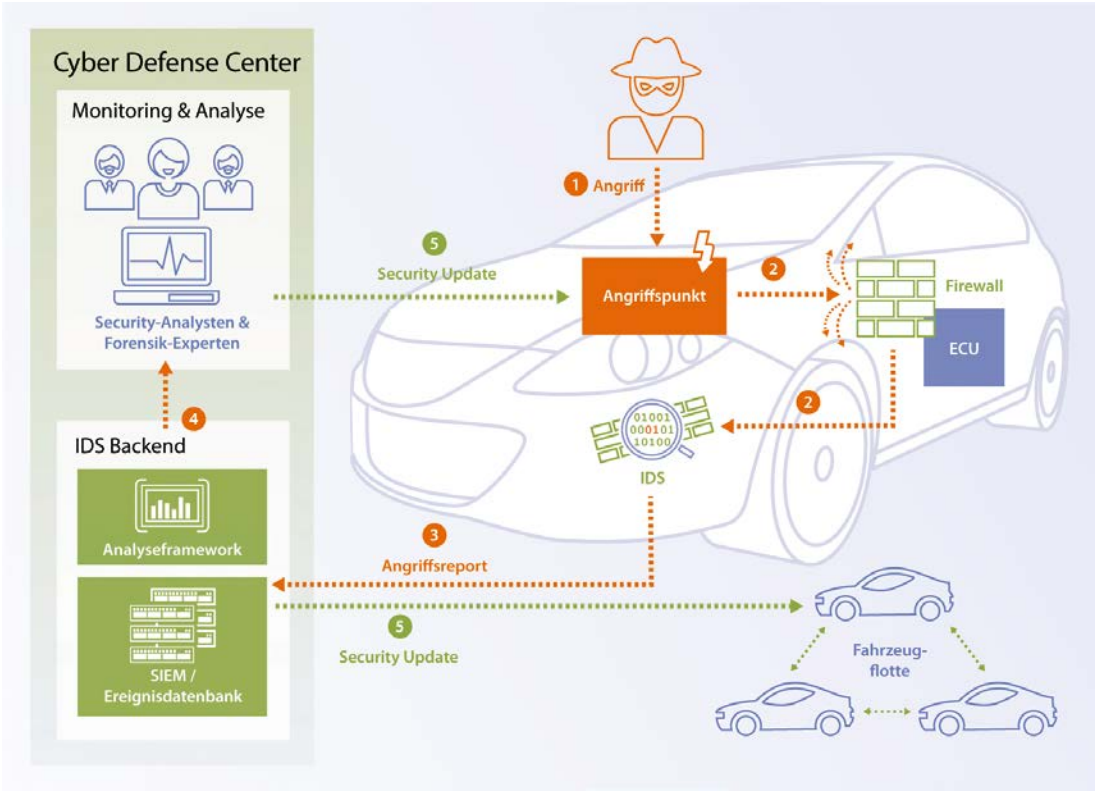

Bild 1: Die Softwarelösung analysiert die Angriffsmuster und nimmt eine Vorsortierung vor, anhand derer dann Sicherheitsexperten und Security-Forensiker entscheiden, ob und welche Gegenmaßnahmen einzuleiten sind. (© Escrypt)

© 2017 Carl Hanser Verlag, München www.hanser-automotive.de Nicht zur Verwendung in Intranet- und Internet-Angeboten sowie elektronischen Verteilern.

matisch Schwachstellen im System – und greifen genau dort an. Es liegt in der Natur der Sache, dass die Existenz dieser Schwachstellen Herstellern in der Regel nicht bewusst ist. Ebenso wenig können Security-Experten alle Angriffsstrategien vorhersehen, die viele Jahre in der Zukunft liegen.

Die klassische IT steht vor ähnlichen Problemen. Auch sie muss IT-Infrastrukturen vor Angriffen schützen, deren Muster noch unbekannt sind. Auch hier versuchen Angreifer Sicherheitsmechanismen auszuhebeln, die bis zu ihrem Angriff als sicher gelten. Schutz bieten in solchen Fällen immer häufiger so genannte intelligente Angriffserkennungs- und Abwehrsysteme (Intrusion Detection and Prevention Systems, IDPS). Bei näherer Betrachtung erscheinen diese Systeme auch dafür prädestiniert, vernetzte Fahrzeuge zu schützen.

Escrypt hat die Technologie darum an die Spezifika der Fahrzeugelektronik und Fahrzeugvernetzung angepasst. Einerseits, damit die Onboard-IDPS-Komponente in den heute gängigen CAN-Netzwerken ebenso wie in künftigen Ethernet-Netzwerken funktioniert. Andererseits galt es, unter automotive-typischen Arbeitsbedingungen mit vergleichsweise geringen Rechnerleistungen volle IDPS-Funktionalität zu gewährleisten. Ein weiterer wichtiger Aspekt war die sinnvolle Lokalisierung der IDPS-Komponente(n) innerhalb der EE-Architektur des Fahrzeugs. Als besonders geeignet erwiesen sich hier die Gateways und zentralen Steuergeräte innerhalb einer Fahrzeugdomäne.

Immunisierung per IDPS

Das Besondere an der IDPS-Technologie: Sie nutzt die Vernetzung der Fahrzeuge, um schneller auf neue Angriffsszenarien reagieren zu können und die daraus resultierenden Abwehrstrategien umgehend an die gesamte Fahrzeugflotte weiterzugeben. So entsteht eine Art Immunsystem, das dynamisch und lernend auf Angriffe reagiert – und in dem jeder Angriff die Abwehrkräfte der Gesamtflotte stärkt.

Im Kern der Intrusion Detection and Prevention Solution (IDPS) von Escrypt steht eine spezielle Security-Software. Sie wacht in Steuergeräten oder Gateways, und analysiert permanent die komplette Bordnetzkommunikation. Tauchen darin Anomalien auf, dann dokumentiert sie diese – und leitet im Fall der Fälle die Abwehr ein. Sofern das erkannte Angriffsmuster schon bekannt ist, blockieren Firewall-Mechanismen die Kommunikation zwischen den verschiedenen Daten-Bussen. Dies ist schon heute Routine.

Doch wird es in Zukunft auch darum gehen, unbekannte Muster und Angriffsstrategien zu erkennen und zu parieren. Dafür müssen u.a. die hinterlegten Regelsets (Black- und White-Lists) ständig auf den neuesten Stand gebracht werden. Genau darin besteht eine Stärke von IDPS. Anomalien und Anzeichen für bisher unbekannte Attacken werden von der neuen Angriffserkennungssoftware detektiert. Diese Software „CycurIDS" ist auf CAN- wie auf künftige Ethernet-basierte EE-Architekturen ausgerichtet und kann die erkannten Anomalien wahlweise im Fahrzeug speichern, um sie zu einem späteren Zeitpunkt auszulesen. Wirksamer ist aber eine Funktion, mit der IDPS die Auffälligkeiten automatisiert in eine Cloud-basierte Event-Datenbank übermittelt. Hier laufen sämtliche Auffälligkeiten aus allen vernetzten Fahrzeugen des Herstellers mit den Fingerprints bereits bekannter Attacken zusammen und können miteinander abgeglichen werden.

Dynamische Schutzstrategie

Aus der Analyse der Daten bekommen OEMs einen umfassenden, stets aktuellen Überblick darüber, welche Strategien Hacker verfolgen, welche Angriffspunkte sie anvisieren und ob sich Attacken häufen. Um diese umfassende Event-Datenbasis in einem Backend auszuwerten, greift die nächste Stufe des dynamischen Abwehrsystems: Die automatisierte auf Big-Data-Methoden basierende Softwarelösung „CycurGUARD". Sie analysiert die Angriffsmuster und nimmt eine Vorsortierung vor, anhand derer dann Sicherheitsexperten und Security-Forensiker eines Cyber-Defense-Centers entscheiden, ob und welche Gegenmaßnahmen einzuleiten sind. Das können gezielte Anpassungen der Firewall sein, Updates des CycurIDS Regelsets – oder die Spezialisten ergreifen in enger Abstimmung mit den Herstellern der betroffenen Steuergeräte Maßnahmen, um die Schwachstellen in deren Software zu beseitigen (Bild 1).

Die getroffenen Maßnahmen können dann over-the-air an alle vernetzten Fahrzeuge der Flotte übermittelt werden. Selbstverständlich geschieht dieser Transfer ausschließlich über kryptographisch abgesicherte Kommunikationsverbindungen. Zusätzlich sind solche Updates mithilfe digitaler Signaturen vor unbemerkten Veränderungen geschützt.

Fazit

Weil sämtliche erkannten Anomalien aus allen Fahrzeugen im Feld in der zentralen Cloud-basierten Event-Datenbank zusammenlaufen, fallen neue Angriffsmuster schnell auf. Mit jedem Fahrzeug, das diesem Verbund angeschlossen ist, wird IDPS intelligenter und abwehrfähiger. Denn indem die bisher unsichtbaren, gegebenenfalls von Firewalls abgeblockten Angriffe in die ständige Lageauswertung einfließen, lassen sich Security-Maßnahmen schneller und gezielter an aktuelle Risiken anpassen. Im Verbund entsteht so ein Immunsystem für das vernetzte Fahrzeug, dessen Abwehrkräfte durch jeden Angriffsversuch gestärkt werden. Die stetig wachsende Datenbasis und die umgehende Weitergabe der Abwehrstrategien an alle Fahrzeuge im Bestand gewährleisten somit einen immer umfassenderen Schutz. ■ (oe)

» **www.escrypt.com**

» **www.hanser-automotive.de/4239393**

Hier finden Sie die Download-Version des Beitrags.

Jan Holle ist Product Manager bei der ESCRYPT GmbH.

© Carl Hanser Verlag, München