Pressemitteilung

ESCRYPT GmbH

Am Hain 5,
44789 Bochum, Deutschland
Telefon: +49 234 43870-200

Presse und Public Relations:
Martin Delle

martin.delle@escrypt.com
www.escrypt.com

Neue Security-Lösung erkennt, analysiert und pariert Cyber-Attacken auf Fahrzeuge im Feld

ESCRYPT präsentiert auf der CES 2018 sein integriertes Intrusion Detection and Prevention System. Mit dem Gesamtsystem aus eingebetteter Lösung und Cyber Defense Center im Backend können Automobilhersteller Cyber-Attacken auf einzelne Fahrzeuge und gesamte Flotten erkennen und abwehren.

Bochum, 08.12.2017 – Machen sich Diebe am Auto zu schaffen, heult im Idealfall die Alarmanlage auf. Wenn nicht, sind nachher zumindest die Einbruchsspuren sichtbar. Dagegen sind unbefugte und kriminelle Angriffe auf IT-Systeme vernetzter Fahrzeuge bisher unsichtbar. Die Folgen können dramatisch sein: Etwa, wenn ein fremdgesteuertes Autoradio plötzlich in voller Lautstärke dröhnt oder persönliche Daten aus angedockten Smartphones entwendet werden. Ganz zu schweigen von Angriffen auf Steuergeräte, die das Fahrzeugverhalten beeinflussen oder gesetzeswidrigen Manipulationen im Antriebssystem.

Automotive Security-Spezialist ESCRYPT hat eine Lösung entwickelt, die Cyber-Angriffe erkennt, analysiert und abwehrt. Die seit 2017 verfügbare Intrusion Detection and Prevention Solution (IDPS) für Fahrzeuge dokumentiert Angriffsversuche und kann die Daten zur Auswertung automatisch an ein Cyber-Security Backend weiterleiten. Dort nutzen Expertenteams die Daten für forensische Analysen der Vorfälle und leiten im Bedarfsfall geeignete Gegenmaßnahmen ein – beispielsweise in Form von over-the-air übertragenen Sicherheitsupdates.

Mit dieser Angriffserkennung und -abwehr wird die Automotive Security zu einem kontinuierlichen Prozess. Dieser reicht von der Prävention (bspw. per Firewall) über das Monitoring und Reporting von Angriffen, bis zu deren Analyse und einem stetigen Roll-out gezielter Gegenmaßnahmen. Anstatt bei statischen Abwehrmaßnahmen im einzelnen Fahrzeug zu verharren, berücksichtigt IDPS also ständig aktualisierte Daten aus der gesamten Fahrzeugflotte und ermöglicht so die umgehende Bereitstellung passender Antworten auf neue – sich ständig verändernde - Risiken und Angriffsstrategien.

Holistischer Ansatz – umgesetzt mit verlässlicher Technik

Ein ganzheitlicher Security-Ansatz ist dringend geboten. Prognosen zufolge werden bis 2021 bereits über 380 Mio. Fahrzeuge vernetzt sein. Bisher geschlossene Fahrzeugsysteme öffnen sich im rasanten Tempo für die Außenwelt. Schnittstellen zu Smartphones und die Möglichkeit zur Car-to-x-Kommunikation bringen neue Risiken an Bord. Zugleich nehmen Steuergeräte und deren Software dem Fahrer immer mehr Verantwortung ab. Automatisiertes Fahren wird real. Diese neue vernetzte Welt erfordert holistische Sicherheitsstrategien, in denen die funktionale Sicherheit und die Automotive Security untrennbar verknüpft sind. Und das über den gesamten Lebenszyklus der Fahrzeuge hinweg. Das beginnt beim Start der Entwicklung, geht mit kryptographisch gesicherter Bedatung der Steuergeräte in der Produktion weiter, gewährleistet einen jederzeit sicheren Fahrzeugbetrieb und endet erst mit dem Löschen kryptographischer Schlüssel und der In-Validierung der Fahrzeugidentität vor der Verschrottung.

ESCRYPT verfolgt solche holistischen Schutzkonzepte seit fast 14 Jahren. Dabei ist IDPS neben Integritätsprüfungen der Steuergerätesoftware, authentifizierter Onboard-Kommunikation sowie die Absicherung verschiedener Fahrzeugdomänen durch Firewalls ein zentraler Baustein des ESCRYPT-Lösungsportfolios. IDPS gewährleistet die IT-Sicherheit vernetzter Fahrzeugen im laufenden Betrieb, rückt also Risiken in den Fokus, die zum Zeitpunkt der Entwicklung und Produktion des Fahrzeugs noch gar nicht

existieren oder noch unbekannt sind.

Angriffserkennung und Angriffsabwehr für Fahrzeuge - IDPS

In der klassischen IT haben sich intelligente Angriffserkennungs- und Abwehrsysteme (Intrusion Detection and Prevention Systems, IDPS) zum Schutz von IT-Infrastruktur in den letzten Jahren bewährt. Die Übertragung dieser Technologie auf das vernetzte Fahrzeug ist dagegen relativ neu. Eine spezielle Security-Software in den zentralen Fahrzeug-Steuergeräten oder Gateways erkennt und dokumentiert Anomalien in der Bordnetzkommunikation.

Erfolgt eine Attacke, dann leitet IDPS eine fünfstufige Abwehrstrategie ein. Ist das Angriffsmuster bekannt, blockt die embedded Firewall CycurGATE Zugriffe auf Steuergeräte sofort ab. Um auch künftige Angriffsstrategien parieren zu können, müssen die hinterlegten Regelsets (Black- und White-Lists) allerdings ständig auf den neuesten Stand gebracht werden. Genau das ist der Kern von IDPS. Anomalien und Anzeichen für eine bisher unbekannte Attacke werden von der neuen Angriffserkennungssoftware CycurIDS detektiert. Diese ist sowohl auf CAN- als auch auf künftige Ethernet-basierte EE-Architekturen ausgerichtet und überwacht den Datenverkehr. Die geloggten Anomalien können im Fahrzeug gespeichert und später ausgelesen werden. Um schnell reagieren zu können, lassen sie sich auch automatisiert in eine Cloud-basierte Event-Datenbank übermitteln. Hier laufen sämtliche Auffälligkeiten aus allen vernetzten Fahrzeugen des Herstellers mit den Fingerprints bereits bekannter Attacken zusammen und können miteinander abgeglichen werden.

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, kommt Stufe vier der Abwehr ins Spiel: CycurGUARD. Diese automatisierte auf Big-Data-Methoden basierende Softwarelösung analysiert die

Angriffsmuster und nimmt eine Vorsortierung vor, anhand derer die Sicherheitsexperten und Daten-Forensiker im Cyber-Defense-Center über die Gegenmaßnahmen entscheiden. Das können gezielte Anpassungen der Firewall sein, Updates des CycurIDS Regelsets oder in enger Abstimmung mit den Herstellern betroffener Steuergeräte auch Maßnahmen zum Schließen von Schwachstellen in deren Software.

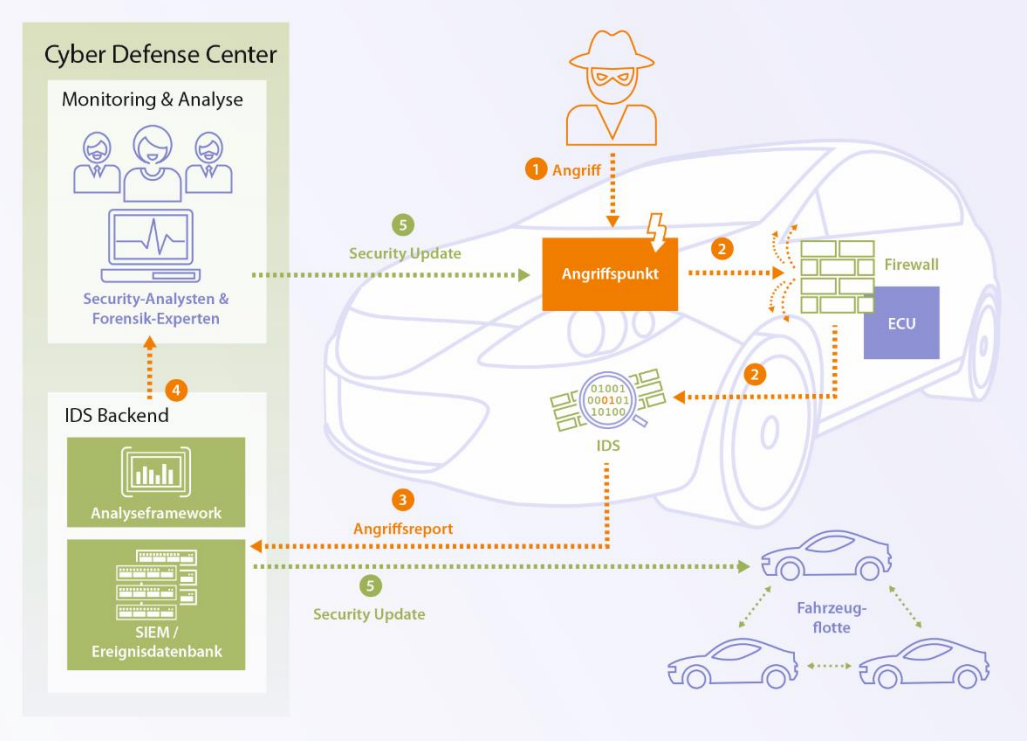
Die Maßnahmen können dann over-the-air an alle vernetzten Fahrzeuge der Flotte übermittelt werden. Dies geschieht natürlich ausschließlich über kryptographisch abgesicherte Kommunikationsverbindungen, und zusätzlich sind die Updates selbst mithilfe digitaler Signaturen vor unbemerkten Veränderungen geschützt. Das komplette Schlüsselmanagement (CycurKEYS) hierfür ist ebenfalls Bestandteil des ESCRYPT Portfolios.

Intelligente Security ruht auf breiter, kontinuierlich aktualisierter Datenbasis
Mit der fünfteiligen Abwehrstrategie schafft IDPS eine zukunftssichere und skalierbare Lösung. Und nicht nur das. Denn mit jedem Fahrzeug im Verbund wachsen die Analysefähigkeiten der Angriffserkennung und damit die Möglichkeiten zur Angriffsabwehr. Jeder bisher unsichtbare – und gegebenenfalls von Firewalls abgeblockte – Angriff hilft, die Security-Maßnahmen gezielt an aktuelle Risiken anzupassen. Anstatt bis zum nächsten Werkstattaufenthalt in Datenspeichern zu ruhen, tragen geloggte und umgehend an das Cyber-Security-Backend übertragene Anomalie-Reports sofort zur Verstärkung des Schutzes bei. Das Connected Car erhält mit IDPS also eine Immunabwehr, die durch Angriffe stärker wird und deren Intelligenz dank der kontinuierlich wachsenden Datenbasis stetig wächst.

Als Pionier in der Automotive-Security nutzt ESCRYPT sein langjähriges Knowhow, um Fahrzeuge auf die tiefgreifenden Veränderungen einer vernetzen Welt vorzubereiten. IDPS versetzt Kunden in die Lage, Abwehrsysteme jederzeit an veränderte Angriffsstrategien und neue Cyber-Risiken anzupassen, statt mit passivem Schutz in der

Defensive zu verharren. Dank ihrer umfangreichen Erfahrungen aus zahlreichen Serienprojekten kann ESCRYPT ihre holistischen Security-Lösungen nahtlos in die Entwicklung und Verifizierung von Steuergeräte-Hard- und Software einbringen. IDPS und Over-the-air-Updates finden somit auf sicheren und etablierten Pfaden ihren Weg in Serienmodelle. Die Spuren digitaler Einbruchsversuche bleiben damit nicht länger unerkannt – sondern können vielmehr zur Verbesserung der Abwehrmaßnahmen genutzt werden.

Intrusion Detection and Prevention - IDPS im Überblick



ESCRYPT GmbH - Embedded Security
Martin Delle
+49 234 43870-290
martin.delle@escrypt.com

ESCRYPT GmbH – Embedded Security
ESCRYPT - Embedded Security ist das führende Systemhaus für eingebettete IT-Sicherheit. An den fünf deutschen Standorten und in den Niederlassungen in Großbritannien, Schweden, in den USA, Kanada, Indien, China, Korea und Japan konzentrieren sich unsere Experten auf aktuelle Datensicherheitsthemen wie sichere M2M-Kommunikation, IT-Sicherheit im Internet der Dinge, Absicherung von E-Business-Modellen und Automotive Security. Hierzu entwickeln sie hochsichere, weltweit geschätzte Produkte und Lösungen, die speziell auf die Anforderungen eingebetteter Systeme und der relevanten IT-Infrastruktur zugeschnitten sind und die sich bereits in der automobilen Serienproduktion millionenfach bewährt haben.
Weitere Informationen finden Sie hier: www.escrypt.com