VDI Wissensforum

Praktische Übungen:
Wenden Sie Praktiken der Hacker selbst an!

Seminar

Automotive Cyber Security für Funk- und Kabelnetze / Over-the-Air-Updates (OTA)

Die Top-Themen:

- **Informationsfluss zwischen Verbraucher, OEM und Fahrzeug**
- **Cyber-Security mobiler Endgeräte (Handy, PC etc.)**
- **Aushebeln der Cyber Security des OEM**
- **Kontrolle über die Funknetze am Fahrzeug**
- **Technische Lösungsansätze für OTA und FOTA**
- **Best Practice - Beispiele**

Termine und Orte

28. und 29. Juni 2022
Stuttgart

25. und 26. Oktober 2022
Berlin

Sicherheitsstrategien für die Datenübertragung von Fahrzeugen - praxisnah vermittelt!

Dipl.-Ing. Jürgen Belz, PROMETO GmbH, Paderborn

Veranstaltung der VDI Wissensforum GmbH
Jetzt online anmelden!
www.vdi-wissensforum.de/01SE183
Telefon +49 211 6214-201 • Fax +49 211 6214-154

Allgemeine Informationen

Zielsetzung

Moderne Fahrzeuge verfügen über deutlich mehr Software als z.B. Verkehrsflugzeuge und müssen regelmäßig Updates erhalten. Kunden sowie Hersteller wünschen sich dabei effiziente und bequeme Wege. Over-the-Air Updates bieten hier eine optimale Lösung – sind aber nicht ohne Risiken vor Hackerangriffen! Genauso wie die Netze der Fahrzeuge geraten sie ins Visier von Hackern.

Die Software der ECUs muss in immer kürzeren Zyklen weiterentwickelt werden, um Fehler zu bereinigen und Verbesserungen umzusetzen. Es gilt, moderne Methoden einzusetzen, die für Updates Funkschnittstellen wie WLAN oder Mobilfunk nutzen. Beim klassischen Over-the-Air (OTA) werden lediglich Einstellungen für einzelne Dienste übertragen. Höhere Anforderungen hat die Firmware Over-the-Air (FOTA). Dabei geht es um das Aufspielen neuer Software auf die ECU. Bei (F)OTA sind teilweise neue Aspekte zu berücksichtigen. Dazu zählt u.a. das wirksame Signieren der Aktualisierungen oder auch das Authentifizieren des Nutzers.
Es gilt hier die Angriffsfläche für Angriffe von außen wirksam zu verringern. Erfahren Sie in diesem VDI-Seminar praxisorientiert, was Sie tun können, um den Schutz Ihrer Software vor unbefugtem Zugriff Dritter bei der Übertragung ins Auto und im Auto sicherzustellen. In ausgesuchten Übungen lernen Sie spielerisch, wie Hacker Netzwerke übernehmen und wie eine gezielte Abwehrstrategie aussehen kann.

Zielgruppe

- Systemingenieure
- Software-Architekten
- Entwickler von Software und Hardware
- Führungskräfte, Projektleiter, Teamleiter aus dem Bereich E/E
- Sicherheitsingenieure und –verantwortliche
- Functional Safety-Manager

bei Fahrzeugherstellern und Zulieferern (Automobil, Mobile Arbeitsmaschinen, NFZ, Bahn, Luftfahrt)

Inhouse-Seminar

Dieses Seminar können Sie auch als firmeninterne Schulung buchen:

Wir erstellen Ihnen gerne ein individuelles Angebot. Rufen Sie uns an.

Frau Angela Bungert/Herr Jens Wilk
Tel.: +49 211 6214-200, E-Mail: inhouse@vdi.de
Herr Heinz Küsters
Tel.: +49 211 6214-278, E-Mail: kuesters@vdi.de

Veranstaltungsdokumentation
Jeder Teilnehmer erhält eine Dokumentation wie Präsentationsunterlagen, Handbuch o.ä. und eine VDI Wissensforum-Teilnahmebescheinigung.

Seminarleitung

Dipl.-Ing. Jürgen Belz, PROMETO GmbH, Paderborn

Nach dem Elektrotechnikstudium, Fachrichtung Automatisierung, leitete Herr Belz die System- und Softwareentwicklung für Hybridfahrzeuge bei Continental. Diese wurde für die „Zukunftsweisende Software-Initiative" mit einem Award ausgezeichnet. Danach war er sieben Jahre weltweit verantwortlich für die Prozesse, Methoden und Werkzeuge in der Hard- und Softwareentwicklung beim Automobilzulieferer Hella. Unter seiner Leitung erreichte Hella als erster Zulieferer den SPICE Level 3 und die Vorstellung des ersten prototypischen AUTOSAR-Steuergerätes, das in einem Fahrzeug verbaut wurde. Seit 2010 ist er Senior Consultant Safety & Security bei PROMETO.
PROMETO ist Anbieter von Dienstleistungen, Infrastrukturen und Technologien zu Embedded-, IT- und Sicherheits-Systemen.

Hinweise

Grundkenntnisse der IT-Security werden vorausgesetzt.
Programmierkenntnisse sind nicht notwendig.

Weitere interessante Veranstaltungen

Automotive Cyber Security Standards
26. und 27. Juli 2022, Hannover
22. und 23. November 2022, Online-Seminar

Cyber Security in Fahrzeugen
02. und 03. August 2022, Düsseldorf
02. und 03. November 2022, Online-Seminar

Seminarinhalte

1. Tag: 09:00 Uhr bis 17:30 Uhr
2. Tag: 08:30 Uhr bis 16:00 Uhr

Einleitung

- Illusion sicherer Software
- Problem eines langen Lebenszyklus
- Risikoquelle Remote Access
- Rechtliche Aspekte
- Statistiken und Schadensbilanzen
- Gezieltes Ausnutzen von Ignoranz und Arroganz
- Dringende Änderung des Mindsets
- Automotive - ein IT-System mit Rädern

Analyse einer End-to-End OTA -Architektur

- Use-cases: Wartung, Updates und Mehrwertdienste
- Geräte im Feld (OEM und 3rd party)
- Öffentliche Netzwerke
- Cloud-Dienste
- Mobile Geräte (Endkunden, Service)
- IT-Netzwerke und Systeme des ECU-Herstellers

Netzwerk-Sicherheit

- Daten in Netzwerken abgreifen
- Ethernet und WLAN Sicherheit
- Datensicherheit in öffentlichen Netzen
- Öffentliche und eigene Zertifikate
- Maßnahme: Verschlüsselung und sichere Passwörter
- Maßnahme: VPN-Verbindungen bevorzugen

Einführung Kryptographie

- Hash-Werte berechnen
- Symmetrische Verfahren
- Asymmetrische Verfahren
- Zertifikate als Berechtigungsnachweis

++ Übung: Remote Dice

Hacking ist auch ein Wettbewerb zwischen Angreifer und Verteidiger. In dieser Übung verteidigen Sie Ihren digitalen Würfel in einem Spiel, der über ein Funknetz angesteuert wird und erleben praxisnahe Angriffstechniken in Funknetzen.

- Funkverkehr abhören
- Funk-Netzwerk übernehmen
- Verschlüsselungsschutz umgehen
- Authentifikation richtig umsetzen

Produktlebenszyklen und System-Design

- Hardware-Lebenszyklus eines Gerätes
- Lebenszyklus für Sicherheitslösungen
- Mechanismen zum Software-Update
- Schlüssel- und Zertifikatsmanagement
- Netzwerk-Sicherheit (Automotive Ethernet, CAN)
- Geeignete Ausrüstung von Mitarbeitern (Notebooks, Handys und andere Mobilgeräte)

++ Übung: CAN Netzwerke

Automotive CAN-Netzwerk mit einem Tacho: Ziel dieser Übung ist es, Schritt für Schritt die erforderlichen Werkzeuge zu bauen, um die Kontrolle über das Netzwerk zu erlangen. Sie erleben aus der Perspektive der Hacker, wie sie ihre Werkzeuge anpassen. Dabei lernen Sie nicht nur effektive Verteidigungsstrategien, sondern auch den Aufbau von kostengünstigen Umgebungen, die sich auch im Entwicklungsumfeld effektiv einsetzen lassen.

- Stärken und Schwächen von AUTOSAR SecOC
- CAN Netze übernehmen
- Aufbau von CAN Hacking- Umgebungen
- Maßnahme: CAN Black & Whitelists

ECU-Design und Anti-Tamper

- Hardware fälschungssicherer gestalten
- Speicher vor Auslesen schützen
- Debug- und Programmier-Schnittstellen vermeiden
- Schlüssel und Zertifikate managen
- Crypto-Chips auswählen
- Secure Boot richtig aufsetzen
- CAN-Netze absichern
- Sichere Netze mit Automotive Ethernet
- Netzwerk-Verbindungen ausreichend verschlüsseln
- Anwender und Sender richtig authentifizieren

Abschlussdiskussion und Ausblick

VDI Wissensforum

Seminar:
Automotive Cyber Security für Funk- und Kabelnetze / Over-the-Air-Updates (OTA)

Jetzt online anmelden
www.vdi-wissensforum. de/
01SE183

Schließen Sie gezielt Sicherheitslücken bei der Datenübertragung!

VDI Wissensforum GmbH | VDI-Platz 1 | 40468 Düsseldorf | Deutschland

Sie haben noch Fragen?
Kontaktieren Sie uns einfach!

VDI Wissensforum GmbH
Kundenzentrum
Postfach 10 11 39
40002 Düsseldorf
Telefon: +49 211 6214-201
Telefax: +49 211 6214-154
E-Mail: wissensforum@vdi.de

www.vdi-wissensforum.de

✓ Ich nehme wie folgt teil (zum Preis p. P. zzgl. MwSt.):

Seminar	
☐ **28. und 29. Juni 2022** **Stuttgart** (01SE183005)	☐ **25. und 26. Oktober 2022** **Berlin** (01SE183006)
EUR 1.590,-	EUR 1.590,-

22H01EM10

☐ Ich bin VDI-Mitglied und erhalte **pro Veranstaltungstag EUR 50,- Rabatt** auf die Teilnahmegebühr: VDI-Mitgliedsnummer*_____

*Für den VDI-Mitglieder-Rabatt ist die Angabe der VDI-Mitgliedsnummer erforderlich.

Meine Kontaktdaten:

Nachname _____ Vorname _____

Titel _____ Funktion/Jobtitel _____ Abteilung/Tätigkeitsbereich _____

Firma/Institut _____

Straße/Postfach _____

PLZ, Ort, Land _____

Telefon _____ Mobil _____ E-Mail _____ Fax _____

Abweichende Rechnungsanschrift _____

_____

Datum Unterschrift

Teilnehmer mit einer Rechnungsanschrift außerhalb Deutschlands, Österreichs oder der Schweiz bitten wir, mit Kreditkarte zu zahlen. Bitte melden Sie sich über www.vdi-wissensforum.de an. Auf unserer Webseite werden Ihre Kreditkartendaten verschlüsselt übertragen, um die Sicherheit Ihrer Daten zu gewährleisten.

Die allgemeinen Geschäftsbedingungen der VDI Wissensforum GmbH finden Sie im Internet: www.vdi-wissensforum.de/de/agb/

Veranstaltungsort(e)
Stuttgart: Mercure Hotel Stuttgart Airport Messe, Eichwiesenring 1/1/, 70567 Stuttgart, Tel. +49 711/7266-0, E-Mail: h1574@accor.com
Berlin: Mercure Hotel Berlin City, Invalidenstr. 38, 10115 Berlin, Tel. +49 30/30826-0, E-Mail: h5341@accor.com

Im Veranstaltungshotel steht Ihnen ein begrenztes **Zimmerkontingent** zu Sonderkonditionen zur Verfügung. Bitte buchen Sie Ihr Zimmer frühzeitig per Telefon oder E-Mail direkt bei dem Hotel mit dem Hinweis auf die „VDI-Veranstaltung". Weitere Hotels in der Nähe des Veranstaltungsortes finden Sie auch über unseren kostenlosen Service von HRS, www.vdi-wissensforum.de/hrs

HRS Das Hotelportal

Leistungen: Im Leistungsumfang ist die Bereitstellung der Veranstaltungsunterlagen enthalten. Bei Präsenzveranstaltungen werden die Pausengetränke und an jedem vollen Veranstaltungstag ein Mittagessen gestellt.

Exklusiv-Angebot: Als Teilnehmer dieser Veranstaltung bieten wir Ihnen eine 3-monatige, kostenfreie VDI-Probemitgliedschaft an (dieses Angebot gilt ausschließlich bei Neuaufnahme).

Datenschutz: Die VDI Wissensforum GmbH verwendet die von Ihnen angegebene E-Mail-Adresse, um Sie regelmäßig über ähnliche Veranstaltungen der VDI Wissensforum GmbH zu informieren. Wenn Sie zukünftig keine Informationen und Angebote mehr erhalten möchten, können Sie der Verwendung Ihrer Daten zu diesem Zweck jederzeit widersprechen. Nutzen Sie dazu die E-Mail Adresse wissensforum@vdi.de oder eine andere der oben angegebenen Kontaktmöglichkeiten.
Auf unsere allgemeinen Informationen zur Verwendung Ihrer Daten auf https://www.vdi-wissensforum.de/datenschutz-print weisen wir hin.
Hiermit bestätige ich die AGBs der VDI Wissensforum GmbH sowie die Richtigkeit der oben angegebenen Daten zur Anmeldung.

Ihre Kontaktdaten haben wir basierend auf Art. 6 Abs. 1 lit. f) DSGVO (berechtigtes Interesse) zu Werbezwecken erhoben. Unser berechtigtes Interesse liegt in der zielgerichteten Auswahl möglicher Interessenten für unsere Veranstaltungen. Mehr Informationen zur Quelle und der Verwendung Ihrer Daten finden Sie hier: www.wissensforum.de/adressquelle

Mit dem FSC® Warenzeichen werden Holzprodukte ausgezeichnet, die aus verantwortungsvoll bewirtschafteten Wäldern stammen, unabhängig zertifiziert nach den strengen Kriterien des Forest Stewardship Council® (FSC). Für den Druck sämtlicher Programme des VDI Wissensforums werden ausschließlich FSC-Papiere verwendet.

FSC www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C124933