Der Scheinwerfer als Sicherheitslücke: Sicherheitsrisiken durch externen Zugriff auf das Fahrzeugnetzwerk

erstellt von

INGENIEURBÜRO BERGER

Tim Berger

Ingenieur für Fahrzeugtechnik M.Eng. - ö.b.u.v. Sachverständiger für Kraftfahrzeugtechnik

Elektronisch gestützte Fahrzeugdiebstähle ersetzen zunehmend klassische Einbruchmethoden und nutzen gezielt Schwachstellen in der Fahrzeugvernetzung aus. Im Rahmen einer technischen Untersuchung wurde an einem Fahrzeug ein sicherheitskritisches Diebstahlszenario nachgestellt, bei dem über das Scheinwerfersteuergerät ein externer Zugriff auf das Fahrzeugnetzwerk erfolgte. Dabei konnte durch den direkten Anschluss eines CAN-kompatiblen Geräts an den Steckverbinder eines Scheinwerfers ein Zugriff auf das Fahrzeugnetzwerk erfolgen. Über diesen Zugang war es möglich, gezielt Steuerbefehle im Fahrzeug zu platzieren und die Zentralverriegelung anzusteuern. Für den Zugriff wurde ein frei im Handel erhältlicher CAN-Datenlogger verwendet, der üblicherweise zu Diagnose- und Entwicklungszwecken eingesetzt wird. Die Untersuchung zeigt exemplarisch, dass nicht abgesicherte Steuergeräte an der Fahrzeugperipherie potenziell kritische Zugriffspunkte darstellen und unterstreicht den dringenden Handlungsbedarf im Bereich der fahrzeugseitigen Netzwerksicherheit.

1. Einleitung

Fahrzeugdiebstähle stellen trotz verbesserter mechanischer und elektronischer Sicherungssysteme weiterhin ein erhebliches sicherheits- und versicherungstechnisches Risiko dar. Die Täter gehen dabei zunehmend professionell und technisch versiert vor. Laut der polizeilichen Kriminalstatistik wurden im Jahr 2023 in Deutschland 13.112 Pkw gestohlen. Besonders betroffen sind dabei hochpreisige Fahrzeuge der oberen Mittel- und Oberklasse, darunter vermehrt Modelle mit sogenannten Keyless-Go-Systemen. Diese Komfortsysteme, die den schlüssellosen Zugang und Motorstart ermöglichen, haben sich in der Praxis als besonders anfällig für elektronische Manipulation erwiesen. Moderne Angriffsmethoden zielen auf Schwachstellen in der Fahrzeugvernetzung, insbesondere im Bereich des CAN-Bus (Controller Area Network). Dieses Kommunikationsprotokoll ist in nahezu allen modernen Kraftfahrzeugen implementiert und ermöglicht den Datenaustausch zwischen elektronischen Steuergeräten (ECUs). Dabei werden sicherheitskritische Komponenten, wie etwa die Motorsteuerung, die Wegfahrsperre oder die Zentralverriegelung, gemeinsam über ein oder mehrere CAN-Teilnetze gesteuert.

Ein zunehmender Angriffstrend ist der direkte Zugriff auf das CAN-Netzwerk über Peripheriekomponenten wie beispielsweise die Scheinwerfer. Diese sind häufig mit komfortbezogenen Steuergeräten ausgestattet, die physisch von außen zugänglich sind, etwa über Radhausschalen oder den vorderen Stoßfänger. Angreifer manipulieren gezielt die Leitungsführung zur Scheinwerfer-ECU, öffnen die Steckverbindung, und schleifen dort ein eigenes Gerät ein. Da viele Fahrzeuge über eine insuffiziente Segmentierung der CAN-Topologie verfügen und auf sichere Authentifizierungsmechanismen zwischen Steuergeräten verzichten, ist es in diesen Fällen möglich, beispielsweise über die Scheinwerferanbindung Zugang zu sicherheitskritischen CAN-Subnetzen zu erlangen. Darüber können, sofern im Fahrzeugnetzwerk keine weiteren Sicherheitsbarrieren implementiert sind, gezielt Nachrichten injiziert werden, etwa zur Entriegelung der Türen oder zur Interaktion mit der Wegfahrsperren. Solche Angriffe setzen keinen physischen Innenraumzugang und auch keine Schlüsselduplizierung voraus.

Die für den Angriff verwendeten Geräte stammen ursprünglich aus dem Umfeld der Fahrzeugdiagnose, Entwicklung oder Tuning-Anwendungen und sind teilweise über frei zugängliche Online-Marktplätze erhältlich. Da sie gezielt Steuergeräte imitieren oder sich nahtlos in den bestehenden CAN-Datenverkehr integrieren, hinterlassen viele dieser Geräte keine digitalen Spuren im Fehlerspeicher des Fahrzeugs. Dadurch ist eine nachträgliche Identifizierung des Angriffs oft nicht möglich, was eine forensische Analyse und eine gerichtsfeste Aufklärung erheblich erschwert.

Aktuelle Untersuchungen zeigen, dass die Schwachstelle nicht in einer spezifischen Komponente liegt, sondern in der Gesamtarchitektur der fahrzeugseitigen Netzwerksicherheit, die häufig noch nicht auf physikalische Angriffe über externe Steuergeräte ausgelegt ist.

2. Verwendete Ausrüstung

Für die Durchführung der Prüfung wurde auf handelsübliche, frei verfügbare Komponenten zurückgegriffen. Im Wesentlichen wurden folgende Komponenten eingesetzt:

- CAN-Logger: Gerät mit Schreibzugriff als Schnittstelle zum Fahrzeug-CAN.
- Adapterkabel: Standard-Adapterkabel zur Verbindung des Loggers mit dem Fahrzeugnetzwerk.
- Spannungsversorgung: Mobile Stromversorgung für den CAN-Logger (7,0 V bis 32,0 V DC).
- CAN-Wake-up-Batterie: Spannungsquelle für den Weckimpuls.
- Sonstige Hilfsmittel: Prüfnadeln oder Tastspitzen zur Kontaktierung einzelner PINs im Scheinwerferstecker sowie ein Taster zur manuellen Auslösung.

Im Ruhezustand (rezessiver Pegel) liegt keine nennenswerte Differenzspannung zwischen CAN-High und CAN-Low vor. Beide Leitungen befinden sich bei etwa 2,5 V, sodass die Differenzspannung rund 0 V beträgt. Im dominanten Zustand hingegen entsteht zwischen den Leitungen eine Differenzspannung von etwa 2,0 V. Wird die Spannung bei aktivem Bus gemessen, zeigt sich entsprechend ein differenzielles Signal von ca. 2,0 V.

Abbildung 1: Angeklemmte PINs am Stecker der Scheinwerfer-ECU.

Zum Aufwecken des CAN-Busses muss ein dominanter Pegel auf die Kommunikationsleitungen gegeben werden. Hierzu werden die Leitungen des Loggers mit dem fahrzeugseitigen CAN-Low und CAN-H verbunden. Zwischen den beiden Leitungen ist ein Spannungsimpulsgeber und ein Tastschalter integriert. Durch Betätigung des Schalters wird ein Spannungssignal erzeugt, das die CAN-Controller aktiviert und den Bus aufweckt. Im Anschluss sendet der Logger die einprogrammierte CAN-Nachricht auf den Datenbus.

3. Zugang zum Scheinwerfersteuergerät

Zur Herstellung der Verbindung wird im vorderen linken Radkasten gearbeitet. Dazu werden Radkasten- und Stoßfängerverkleidung im vorderen Bereich gelöst, bis ein Zugang zum Scheinwerfer möglich ist, auf dessen Unterseite das Scheinwerfersteuergerät angeordnet ist. Zur Kommunikation mit dem CAN-Bus werden Prüfspitzen in die jeweiligen Pins des Steuergerätesteckers eingeführt. Anschließend wird das Adapterkabel mit dem CAN-Logger verbunden. Nach kurzer Initialisierung zeigen zwei LEDs die Betriebsbereitschaft an.

Abbildung 2: Der Tastendruck löst den Spannungsimpuls aus.

4. Entriegelung der Fahrertür

Als Folge der Tasterbetätigung sendet der CAN-Logger über die Steckverbindung des Scheinwerfer-Steuergeräts eine gezielte CAN-Nachricht an das im Fahrzeug-CAN-Netzwerk integrierte Karosseriesteuergerät. Dieses interpretiert die empfangene Nachricht als Steuerbefehl zur Ansteuerung des Verriegelungsmotors der Fahrertür. Dadurch wird der Verriegelungsmechanismus ausgelöst, wodurch die Tür entriegelt wird.

Abbildung 3: Nach dem Senden der Nachricht wird die Fahrertür entriegelt.

5. Zusammenfassung

Im Rahmen der Untersuchung wurde geprüft, ob ein Zugriff auf den CAN-Bus über den Scheinwerferstecker möglich ist. Es konnte bestätigt werden, dass ein unbefugtes Eindringen in das Fahrzeug mittels frei verfügbarer Werkzeuge innerhalb kurzer Zeit realisierbar ist. Dabei wurde die Fahrertür durch das Senden einer gezielten CAN-Nachricht über den Scheinwerfer-ECU-Stecker entriegelt. Die Nachricht wurde von der Hauptkarosserie-ECU empfangen, welche das Signal zur Türentriegelung an den entsprechenden Stellmotor weiterleitete.

Die gemeinsame Einbindung sicherheitskritischer Steuergeräte sowie des extern zugänglichen Scheinwerfersteuergeräts auf demselben Subnetz stellt ein erhebliches Sicherheitsrisiko dar. Besonders kritisch ist dabei die Integration der Zertifizierungs-ECU, welche im gleichen Subnetz wichtige Kommunikationsfunktionen zur Wegfahrsperre und zum Hybridsteuergerät verwaltet. Über diesen Zugang kann im Extremfall der Fahrzeugstart freigegeben werden.

Zur Vermeidung solcher Sicherheitslücken wird empfohlen, bestehende Fahrzeugmodelle mit einer zusätzlichen Wegfahrsperre nachzurüsten. Für künftige Fahrzeuggenerationen sollten erweiterte Sicherheitsmechanismen implementiert werden, darunter:

- Netzwerkarchitektur: Sicherheitsrelevante Steuergeräte in nicht von außen zugänglichen Subnetzen platzieren.
- Physikalische Sicherheit: Physische Zugangskontrollen zur Verhinderung unbefugten Zugriffs auf CAN-Knoten.
- Autorisierung: Einsatz von Nachrichtenauthentifizierungscodes, Beschränkung der Nachrichtenübermittlung auf autorisierte Geräte und IDs sowie rollenspezifische Zugriffsrechte.
- Verschlüsselung: Ende-zu-Ende-Verschlüsselung von CAN-Nachrichten.
- Nachrichtenfilterung und IDS: Implementierung von Nachrichtenfiltern und Intrusion Detection Systemen zur Erkennung und Abwehr ungewöhnlicher Netzwerkaktivitäten.

Die Untersuchung zeigt deutlich, dass ein Zugriff auf sicherheitsrelevante Fahrzeugfunktionen über von außen erreichbare Komponenten wie den Scheinwerferstecker möglich ist. Die Integration der Steuergeräte in ein gemeinsames Subnetz ohne ausreichende physikalische und logische Absicherung stellt dabei ein erhebliches Risiko dar. Besonders kritisch ist die Anbindung der Zertifizierungs-ECU, die als zentrales Element der Wegfahrsperre fungiert und somit indirekt den Fahrzeugstart beeinflussen kann. Insgesamt verdeutlicht die Analyse die Notwendigkeit, bereits in der Entwicklungsphase sicherheitskritischer Systeme ein hohes Maß an IT-Sicherheit zu gewährleisten, um moderne Fahrzeuge wirksam vor Manipulation und unbefugtem Zugriff zu schützen.

Trier, im März 2024

Das in diesem Bericht dargestellte Fallbeispiel basiert auf anonymisierten Inhalten aus der gutachterlichen Praxis. Rückschlüsse auf konkrete Verfahren, Personen oder Fahrzeuge sind nicht möglich. Die technische Bewertung wurde für den Bericht abstrahiert und spiegelt nicht notwendigerweise die vollständige Sachverhaltsdarstellung aus dem Originalgutachten wider.