

Sechs Millionen Teslas ohne UWB: Salzburger App schließt Lücke im Bluetooth-Autoschlüssel

Urstein bei Salzburg — Die toothR new media GmbH, ein österreichisches IT-Sicherheitsunternehmen im Wissenspark Urstein bei Salzburg, das unter der Marke IT-Wachdienst.com kleine und mittlere Unternehmen berät, veröffentlicht die Android-App **TeslaKee**. Sie entschärft zwei dokumentierte Schwachstellen des Bluetooth-Autoschlüssels von Tesla.

Relay-Angriff: Zwei Täter verlängern mit handelsüblichen Funkmodulen die Bluetooth-Strecke zwischen dem Telefon der Besitzerin und dem geparkten Fahrzeug. Das Auto entriegelt und lässt sich wegfahren, während das Telefon unberührt in der Jackentasche steckt — ohne Einbruchsspuren. Neuere Fahrzeuge wehren das per UWB-Distanzmessung ab. Von den weltweit rund acht Millionen Tesla mit Bluetooth-PhoneKey verfügen jedoch nur etwa 20 Prozent über UWB; für **rund sechs Millionen Fahrzeuge** bleibt die Lücke offen.

BlueBait-Attacke: Die offizielle App antwortet auch gefälschten Fahrzeugen. Ein nachgebauter Tesla-Beacon für wenige Euro genügt, um festzustellen, dass eine bestimmte Person zu einer bestimmten Zeit an einem bestimmten Ort war — unabhängig davon, wo ihr Auto steht. Mehrere solcher Beacons ergeben ein Bewegungsprofil, nutzbar für Stalking, verdeckte Beobachtung oder die Vorbereitung eines Diebstahls. **Gegen diesen Angriff hilft auch UWB nicht.**

Beide Schwachstellen sind seit ihrer Erstpräsentation auf der CanSecWest 2022 in Vancouver öffentlich dokumentiert und bis heute offen; neue Angriffsdetails werden nicht offengelegt. Neu ist die Gegenmaßnahme: TeslaKee schaltet eine **Policy-Engine** vor jede Antwort des Telefons: Erst wenn Bewegung, Standort, WLAN, Tageszeit oder Signalstärke zu einer plausiblen Annäherung an das eigene Auto passen, wird geantwortet — sonst schweigt die App, und beide Angriffe laufen ins Leere. Häufige Aufgaben wie Ver- und Entriegeln, Fenster, Laden und Klima lassen sich direkt in der App erledigen, ein **Auto-Sentry-Modus** aktiviert die Fahrzeugüberwachung automatisch außerhalb vertrauter Parkorte. Die App **kommt ohne Internetverbindung, Konto und Cloud aus**; die Schlüssel entstehen im Sicherheitschip des Telefons und verlassen ihn nie. Die offizielle Tesla-App wird nicht ersetzt, sondern ergänzt — beide laufen parallel.

TeslaKee ist ab sofort für Android ab Version 10 verfügbar: <https://play.google.com/store/apps/details?id=com.teslakee.teslakee> — Grundfunktionen sind kostenlos, Premium kostet 2,99 € monatlich oder 29,99 € jährlich. Eine iPhone-Version ist in Arbeit.

Wie sichtbar das eigene Fahrzeug per Bluetooth ist, lässt sich mit der kostenlosen Beobachtungs-App Tesla Radar desselben Anbieters selbst nachprüfen: <https://play.google.com/store/apps/details?id=com.toothr.teslaradar>. Technische Dokumentation der BlueBait-Attacke: <https://trifinite.org/stuff/bluebait/>

Pressekontakt: DI (FH) Martin Herfurt, IT-Sicherheitsberater · toothR new media GmbH · Marke IT-Wachdienst.com · Urstein Süd 15, 5412 Puch bei Hallein · +43 676 3787909 · presse@it-

wachdienst.com · it-wachdienst.com · teslakee.com

Unabhängiges Unternehmen, nicht von Tesla, Inc. autorisiert oder gesponsert. Langfassung, Bildmaterial und Live-Demonstration auf Anfrage.