See no evil – Angriffe auf autonome Fahrzeuge und deren Strafbarkeit

RA Stefan Hessel

Associate im Team Datenschutz & Cybersecurity bei reuschlaw Legal Consultants in Saarbrücken

Dipl.-Jur. Lena Leffer

Wissenschaftliche Mitarbeiterin, Professur für Rechtsinformatik, Universität des Saarlandes und Stationsreferendarin bei reuschlaw Legal Consultants in Saarbrücken

Dipl.-Jur. Karin Potel

Wissenschaftliche Mitarbeiterin, Professur für Rechtsinformatik, Universität des Saarlandes und Stationsreferendarin bei reuschlaw Legal Consultants in Saarbrücken

Agenda

- Problemstellung
- Stufen der Automatisierung
- Bedeutung der Sensorik
- Angriffsmöglichkeiten
  - Ausnutzen von Adversarial Learning
  - Manipulation durch Projektion
- Rechtliche Betrachtung
- Fazit

Problemstellung

6. November 2019, 11:53 Uhr Uber

Tödlicher Unfall: Robotaxi hatte Software-Fehler

Uber ist eines von mehreren Dutzend Unternehmen, die eigene Systeme für autonom fahrende Autos entwickeln und auf öffentlichen Straßen in den USA testen. (Foto: Angelo Merendino, AFP)

Problemstellung

6. November 2019, 11:53 Uhr Uber

Tödlicher Unfall: Robotaxi hatte
are-Fehler

BER

, die eigene Systeme für autonom fahrende Autos
A testen. (Foto: Angelo Merendino, AFP)

US-BEHÖRDEN UNTERSUCHEN TESLA-UNFALL

Erster Toter in selbstfahrendem Auto

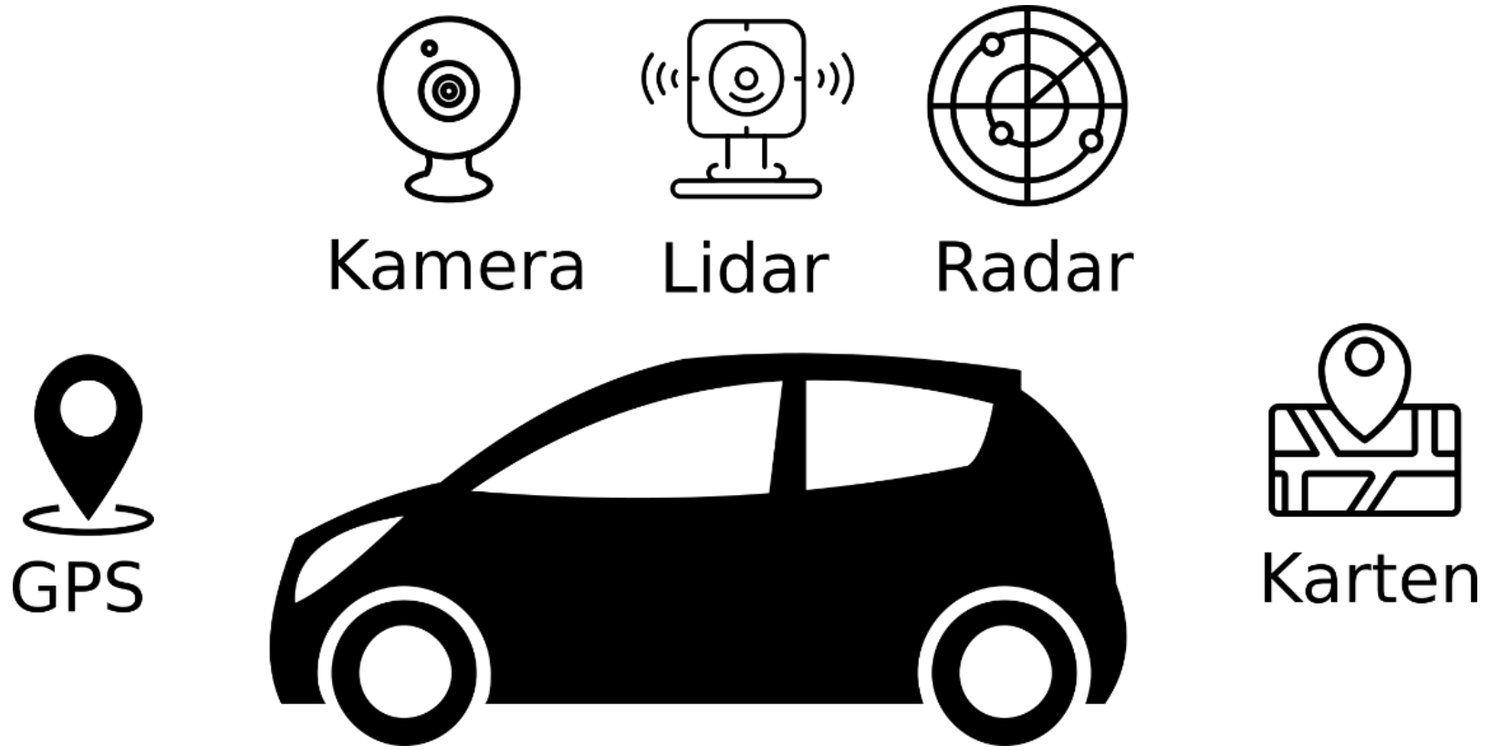
Die US-Verkehrsaufsicht untersucht einen tödlichen Unfall mit einem Tesla-Elektroauto. Ein Mann starb, als der Wagen auf Autopilot geschaltet war. Stellt die Behörde Mängel fest, könnte dies eine Rückrufaktion auslösen.

30.06.2016 • Update: 01.07.2016 - 06:31 Uhr • 24 x geteilt

Stufen der Automatisierung

- Assistiertes Fahren
- Teilautomatisiertes Fahren
- Hochautomatisiertes Fahren
- Vollautomatisiertes Fahren

Bedeutung der Sensorik



Angriffsmöglichkeiten

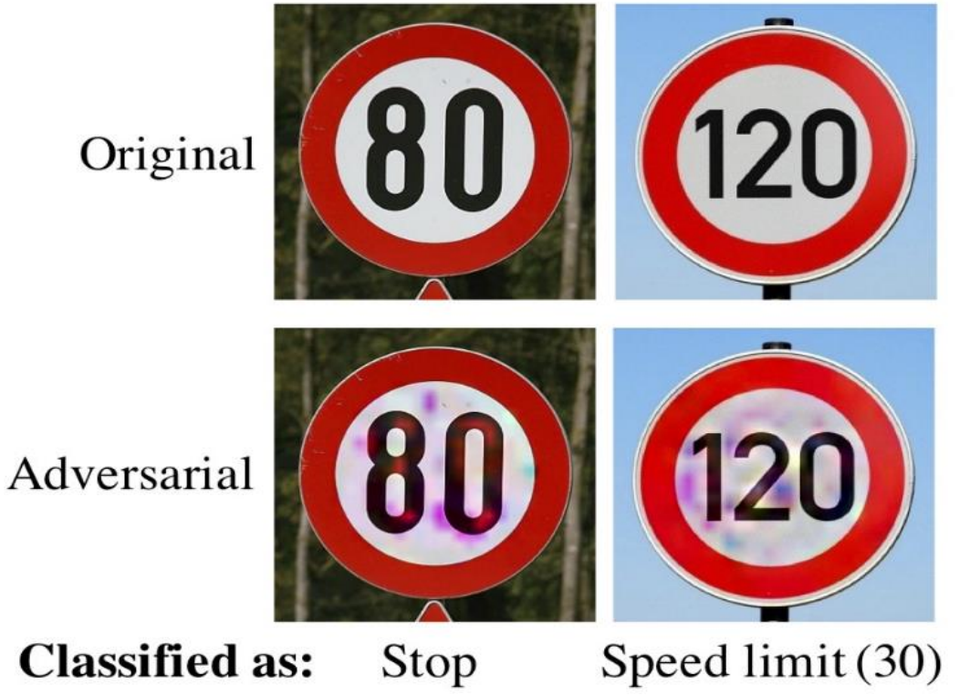
- Ausnutzen von Adversarial Learning
- Manipulation durch Projektion

Angriffsmöglichkeiten

- Ausnutzen von Adversarial Learning
  - Angriffe auf maschinelles Lernen
  - Angreifer modifiziert die Muster eines Objekts so, dass Wahrscheinlichkeit der korrekten Erkennung sinkt, sogar falsche Klassifizierung möglich
  - Modifizierung für das menschliche Auge nicht erkennbar

Angriffsmöglichkeiten

- Ausnutzen von Adversarial Learning

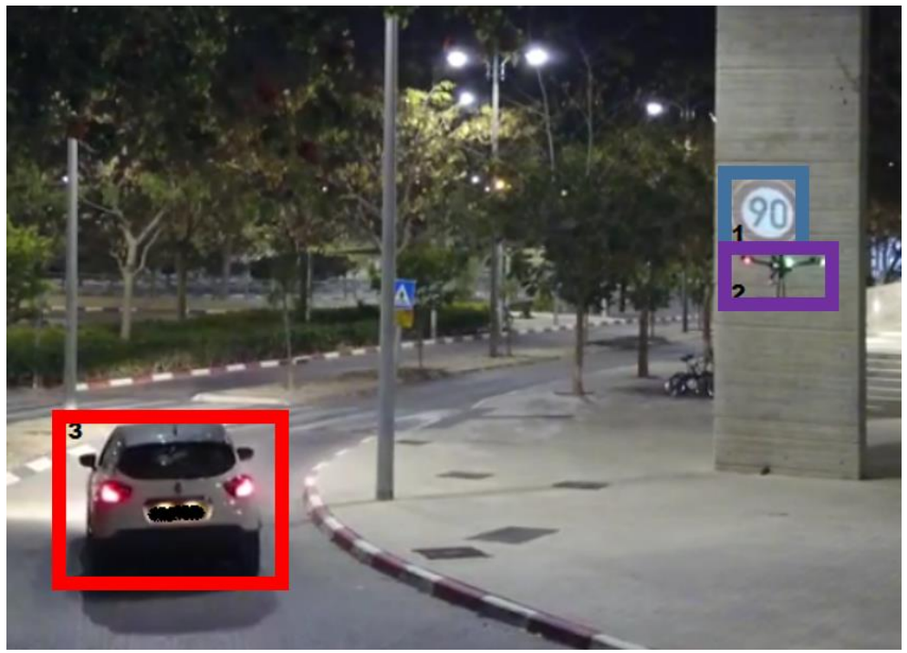


Angriffsmöglichkeiten

- Manipulation durch Projektion
  - Assistenzsysteme können Verkehrszeichen erkennen
  - Täuschung über Höchstgeschwindigkeit durch Projektion eines Verkehrszeichens an eine Hauswand gelungen
  - Projektion für das menschliche Auge erkennbar

Angriffsmöglichkeiten

- Manipulation durch Projektion



Rechtliche Betrachtung

- Urkundenfälschung

Adversarial Learning	Manipulation durch Projektion
• Verkehrszeichen ≠ Urkunde • Auch fehlt es an einer tauglichen Tathandlung	

Rechtliche Betrachtung

- (gemeinschädliche) Sachbeschädigung

Adversarial Learning	Manipulation durch Projektion
Verkehrszeichen dient öffentlichem Nutzen → Taugliches Tatobjekt des § 304 StGB	
Abs. 1: Funktions-beeinträchtigung → **Strafbarkeit** Abs. 2: subsidiär	Abs. 1: keine Einwirkung auf die Sache Abs. 2: Projektion ≠ dauerhafte Veränderung

Rechtliche Betrachtung

- Gefährliche Eingriffe in den Straßenverkehr

Adversarial Learning	Manipulation durch Projektion
Verkehrszeichen = Anlagen i.S.d. § 315b StGB	
1. Abstrakte Gefahr durch Manipulation 2. Eintritt einer konkreten Gefahr im Einzelfall („Beinahe-Unfall“) → Eingriffspflicht des Fahrers?	

Rechtliche Betrachtung

- Amtsanmaßung

Adversarial Learning	Manipulation durch Projektion
Aufstellen eines Verkehrszeichens nur kraft öffentlichen Amtes, § 45 StVO Ausreichend: objektiver Anschein einer Amtshandlung	
Problem: maschinelle Wahrnehmung	Verwechslung eher unwahrscheinlich Ausnahme: Ort, Qualität

Fazit

- Gezielte Angriffe als neue Gefahrenquelle
- Strafrecht ist Herausforderungen derzeit gewachsen
- Tätigkeit des Gesetzgebers bei etwaigen Strafbarkeitslücken erforderlich

Kontakt

- reuschlaw.de
- legalinf.de/leffer
- legalinf.de/potel

- stefan.hessel@reuschlaw.de
- lena.leffer@uni-saarland.de
- karin.potel@uni-saarland.de

- @stefan_hessel
- @LefferLena
- @KarinPotel