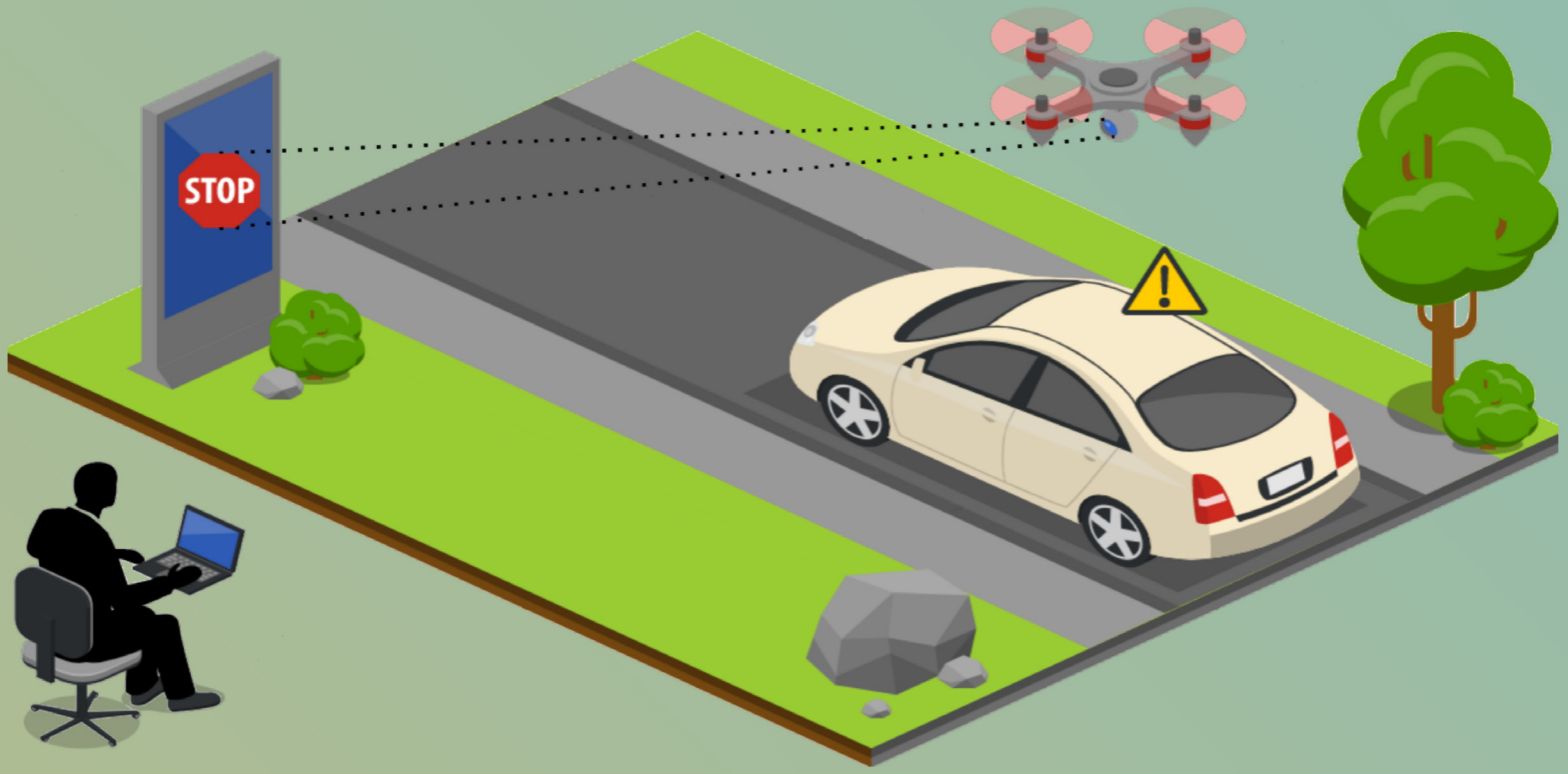
TECHNISCHE HOCHSCHULE DEGGENDORF



SKINET

DURCH DIE ANWENDUNG VON METHODEN DER KÜNSTLICHEN INTELLIGENZ WERDEN IM SKINET PROJEKT ANGRIFFE, Z.B. AUF DAS FAHRER-ASSISTENZSYSTEM EINES FAHRZEUGS, DETEKTIERT UND ABGEWEHRT.

SKINET

Weitere Infos

Abstract

Projekttitel/ Project title:

Proaktive Sicherheit durch Künstliche Intelligenz in automobilen und industriellen IT-Netzwerken (SKINET)

Einleitung/ Introduction:

Durch die ständig zunehmende Vernetzung in Industrie, kritischer Infrastruktur, privaten Haushalten und im Verkehrswesen nimmt die potentielle Angriffsoberfläche auf IT-Systeme rasant zu. Beispiele aus der Vergangeinheit wie WannaCry haben gezeigt, dass Attacken auf die verknüpfte IT-Welt folgenschwere Auswirkungen auf kritische Infrastruktur wie Krankenhäuser, etc. haben kann.

Diese Konnektivität bietet Nutzern und Betreibern auch die Möglichkeit einer verteilten und auf künstlicher Intelligenz (KI) basierender Anomalieerkennung. Anomalien stellen hierbei Datenstrukturen dar, die von maliziösen Akteuren durch Cyberangriffe in ein System gelangt sind.

Ziel/ Aim:

Das Ziel des SKINET-Projekts beinhaltet das Schützen von industriellen und automotive Entitäten vor möglichen Cyberangriffen. Hierbei werden *KI-Agenten* in verschiedene Knoten eines Netzwerks integriert, die durch die Anwendung von auf KI basierenden Algorithmen Anomalien extrahieren.

Da üblicherweise eine bestehende Kommunikation aus einer Fülle an Netzwerkpaketen besteht, bieten Algorithmen aus der künstlichen Intelligenz eine besonders gute Lösung, da mit diesen automatisiert eine Vielzahl an Daten verarbeitet werden kann. Somit kann der Datenaustausch durch diese Operationen vorgefiltert und durch einen Mitarbeiter einer Security Information and Event Management (SIEM) bearbeitet werden. Ziel des Projekts ist neben der Erkennung von malizösen Pakten auch autonom durchzuführende Reaktionsmechansimen der KI-Agenten. Hierbei sollen potentielle Reaktionsmechanimen in Abhängigkeit der Angriffsart eigenständig ausgewählt und ausgeführt werden.

Im SKINET-Projekt werden die Anwendungsfälle aus Industrie und Automobilgenre differenziert betrachtet. Da die Anforderungen an die Szenarios grundlegend unterschiedlich sind, müssen diese in zwei gesonderten Fällen ausgearbeitet werden. Im Folgenden wird eine spezielle Angriffsart auf ein automotive System beschrieben.

Methode/ Method:

Phantomangriffe auf die Fahrerassistenzfunktion:
Ein Beispiel eines Angriffes auf ein autonom agierendes Fahrzeug ist der Angriff mittels Phantomen. Phantome stellen Projektionen von Gegenständen dar, die die Objekterkennung von autonomen Fahrzeugen negativ beeinflussen und eine unnötige Reaktion hervorrufen sollen. So könnte z.B. ein maliziöser Akteur die zu erkennende Geschwindigkeitsbegrenzung eines Fahrzeuges täuschen, indem Schilder

mit einer höheren Geschwindigkeitsbegrenzung im Aufnahmebereich der Objekterkennung projeziert werden. Um dies zu verhindern werden neuronale Netze basierend auf einer mathematischen Operation, der Faltung, implementiert, die durch diese Operation spezielle Merkmale der Projektionen extrahieren und aufgrund deren eine Bewertung der Echtheit durchführen kann.

Ergebnis/ Result:

Das zu erreichende Ziel ist der Schutz von Netzwerken aus dem automotive und industrial Usecase. Spezifische Ergebnisse sind aufgrund des jungen zeitlichen Fortschritts noch nicht vorhanden.

Projektbeteiligte/ Project participants:

Andreas Urmann, Amar Almaini

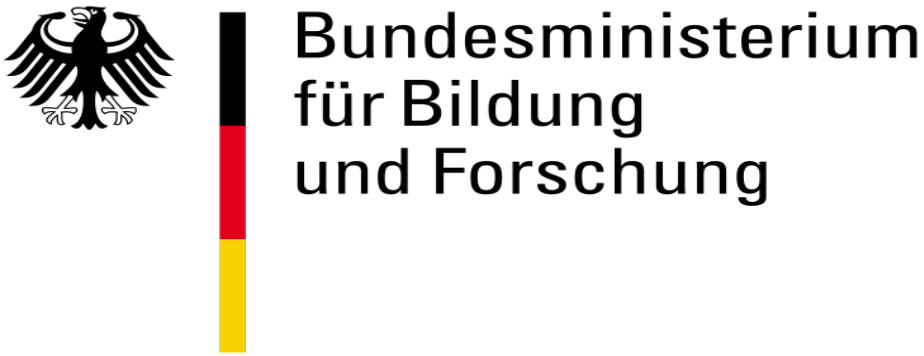
Projektpartner/ Project partners:

AVL, B+, TG-Alpha, Carl Zeiss AG, TU München

Gefördert durch/ Funded by:

Bundesministerium für Bildung und Forschung

Logos/ Logos:



insgesamt maximal 450 Wörter/ limit of 450 words in total