WARUM THREATGET?

Unsere Gesellschaft befindet sich derzeit in einer Phase der Digitalisierung, verschiedenste Alltagsgeräte werden zunehmend vernetzt (Internet of Things, IoT). Ein beliebtes Beispiel dafür ist das Smart Home. Weltweit bieten Hersteller heute viele Möglichkeiten an, um unser Zuhause zu vernetzen und in die digitale Welt einzubinden. Bisher geht dieser Trend jedoch mit einem ganz zentralen Makel einher: einem fehlenden Sicherheitskonzept. Das wird Nutzer*innen allerdings erst dann schmerzlich bewusst, wenn z.B. durch einen unerlaubten Zugriff auf das eigene Netzwerk Schaden entstanden ist. Hier fehlen also Methoden, Konzepte und spezielle Sicherheitsarchitekturen, die diese digitale Vernetzung zuverlässig und vor allem sicher vor unberechtigtem Zugriff von außen machen können.

LieberLieber

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Was beim vernetzten Kühlschrank vielleicht noch durch die einfache Entkopplung vom Hausnetzwerk gelöst werden kann, wird im Auto plötzlich viel kritischer oder sogar lebensbedrohend. Im Kontext des automatisierten Fahrens prognostizieren Hersteller in Zukunft eine enge Vernetzung der Fahrzeuge. Bereits heute sind Autos mit dem Internet verbunden, um Softwareupdates (Navigationssysteme, Bordcomputer etc.) zu ermöglichen. Auch verfügen seit letztem Jahr in der EU alle Neufahrzeuge über ein System, das bei einem Unfall automatisch einen Notruf auslöst (eCall).

Dabei setzen immer mehr Hersteller auf Kommunikationsverbindungen über das Internet, um eine Fahrzeugkommunikation in beide Richtungen zu ermöglichen. Nur so lassen sich nämlich mittels Update einfach neue Funktionen einspielen oder raschere Hilfe im Falle einer Panne über z.B. ein Remote-Auslesen von Motorzuständen durch die Werkstatt realisieren. Allerdings ergibt sich dabei dieselbe Sicherheitsproblematik wie im Smart Home Beispiel. Das so entstehende Gefahrenpotential ist im Auto jedoch wesentlich größer als im Smart Home.

So mehren sich schon heute Nachrichten über gehackte Fahrzeuge, wobei gerade Premium-Autos durch ihre vielfältigen digitalen Funktionen besonders betroffen sind. So berichtete etwa das Magazin AutoBild (Artikel „BMW Software weiter angreifbar“) über Recherchen des ADAC zu einer speziellen Softwarelücke bei BMW. Diese erlaubte es, via Laptop Autos zu öffnen, indem Signale der Funkschlüssel mobil umgeleitet wurden. Dadurch konnte man sich Zugriff auf das Fahrzeug verschaffen, obwohl der Fahrzeugbesitzer selbst während der Entsperrung nicht neben dem Auto stand.

Wäre dieses Szenario bereits in der Designphase des Fahrzeugs berücksichtig worden, dann wäre diese Lücke erst gar nicht aufgetreten. Über die Messung der Laufzeit lässt sich nämlich einfach feststellen, dass das umgeleitete Signal mit dem Befehl der Fahrzeugentsperrung nicht direkt vom Funkschlüssel, sondern über ein Drittgerät durchgeführt wird. Nun könnte man annehmen, ein Fahrzeug ließe sich einfach so programmieren, dass es sich – nachdem ein Einbrecher ohne Schlüssel damit weggefahren ist – nach einer gewissen Entfernung zum Schlüssel einfach selbst deaktiviert. Das würde jedoch ein enormes Sicherheitsrisiko im Straßenverkehr bedeuten – man denke z.B. an die Deaktivierung von Servolenkung, Lenkradsperre oder Bremskraftverstärker, während sich das Fahrzeug auf der Autobahn bewegt. Da dies ein viel zu hohes Sicherheitsrisiko auch für andere Verkehrsteilnehmer darstellen würde, muss diese Problemstellung bereits sicherheitstechnisch und im Sicherheitskonzept zeitlich vor der Fahrzeugentsperrung berücksichtigt und gelöst sein.

Fazit: gerade vernetzte Autos stellen eine äußerst sicherheitskritische Infrastruktur dar. Daher muss bereits vor dem Aufbau eines Systems zum automatisierten Fahren eine spezielle Sicherheitsarchitektur entwickelt werden, um den Verkehr zuverlässig und sicher gestalten zu können.

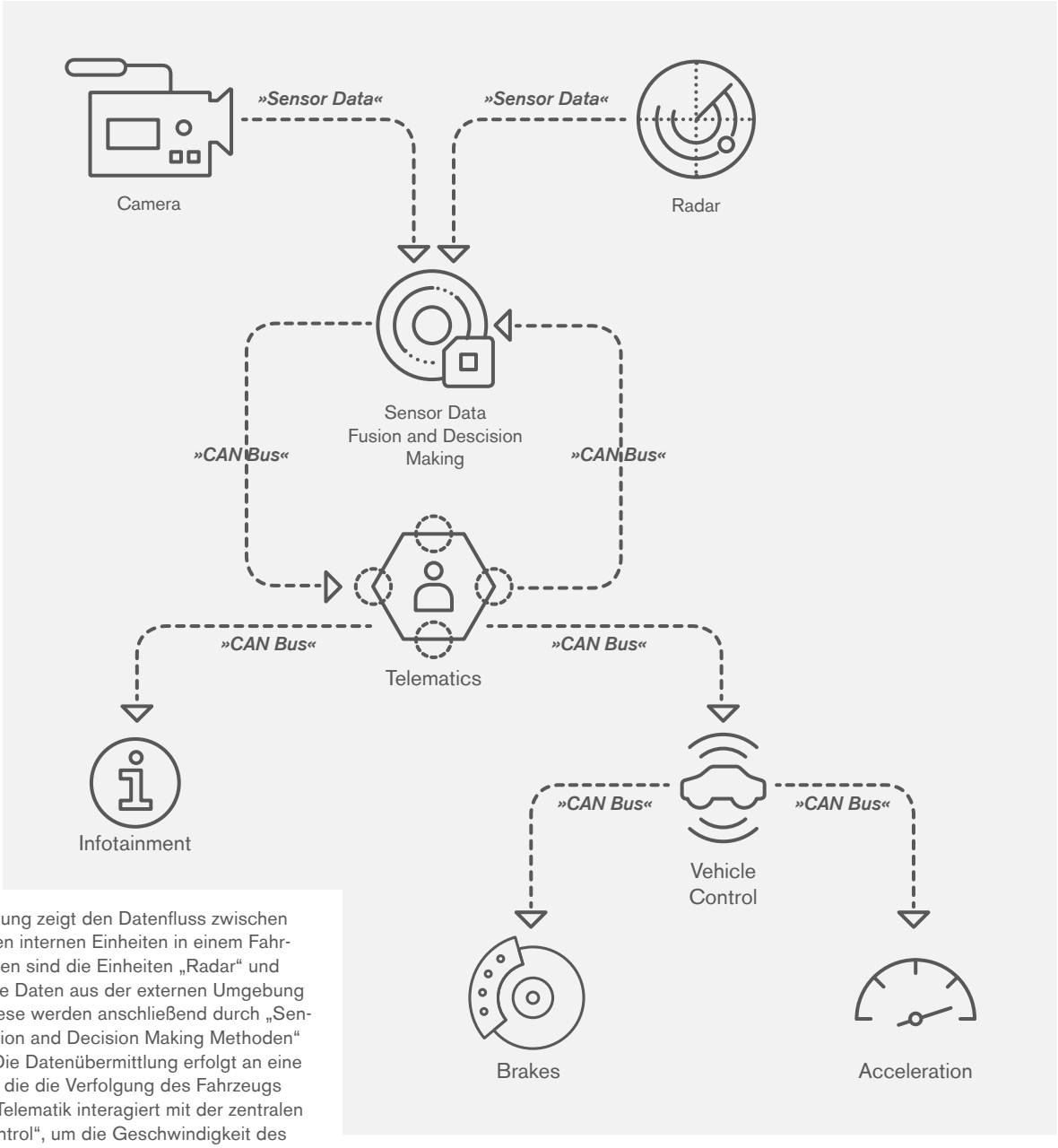
NEUE RICHTLINIEN – CYBERSICHERHEIT WIRD ZUR VORAUSSETZUNG FÜR DIE ZULASSUNG

Angesichts der dargestellten besonderen Relevanz eines umfassenden Sicherheitskonzepts stellt sich nun die Frage: Warum wird das nicht bereits gemacht? Die Antwort ist einfach – weil sich Hersteller bisher auf ihren Kosten-Nutzen-Standpunkt zurückziehen und auf entsprechende Versicherungen verweisen konnten. Doch mit der neuen europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie; https://www.cert.at/reports/report_2016_chap04/content.html) ändert sich diese bisher allgemein übliche Herangehensweise grundlegend.

Speziell mit der Einführung der neuen Europäischen Sicherheitsrichtlinie nach ECE Level (UNECE WP29; gilt in der EU und teilweise in Asien) wird Fahrzeugherstellern künftig vorgeschrieben, die Cybersicherheit ihrer Fahrzeugsysteme nachweislich zu überprüfen, um eine Zulassung ihrer Produkte zu erhalten. Hersteller

Hersteller müssen ab nun alle drei Jahre nachweisen, dass sie ein zertifiziertes Cyber-Security-Management-System einsetzen, das alle Stationen vom Fahrzeug-Engineering bis hin zur - Dokumentation berücksichtigt. Mit diesem Cyber-Security-Management-System müssen sie:

- alle Fahrzeugtypen auf Cybersicherheit überprüfen,
- das mögliche Bedrohungspotential identifizieren und dokumentieren und
- sicherheitskritische Probleme mit Lösungsvorschlägen adressieren und nachweislich lösen.



Diese Abbildung zeigt den Datenfluss zwischen verschiedenen internen Einheiten in einem Fahrzeug. Zu sehen sind die Einheiten „Radar“ und „Camera“, die Daten aus der externen Umgebung sammeln. Diese werden anschließend durch „Sensor Data Fusion and Decision Making Methoden“ verarbeitet. Die Datenübermittlung erfolgt an eine „Telematics“, die die Verfolgung des Fahrzeugs steuert. Die Telematik interagiert mit der zentralen „ Vehicle Control“, um die Geschwindigkeit des Fahrzeugs entweder durch “Brakes“ oder durch “Acceleration“ zu steuern. Das „Infotainment“ verbindet sich mit der Telematikeinheit, um dem Fahrer Informationen zur Verfügung zu stellen.
(Alle Grafiken: AIT)

PRODUKTLAUNCH UND ZIELGRUPPEN VON THREATGET

Voraussetzung für diese Cybersicherheitsüberprüfung ist ein modernes Werkzeug, dass die Hersteller überhaupt erst dazu befähigt, ihre Systeme ECE-Level-konform zu überprüfen. Dazu hat das AIT Austrian Institute of Technology eine Lösung namens THREATGET entwickelt, das auf einem laufend gewarteten Katalog mit Bedrohungspotential für den Automotive-Sektor aufbaut. Gemeinsam mit dem österreichischen Unternehmen LieberLieber Software GmbH wurde THREATGET zum Produkt weiterentwickelt und nun erstmals der Öffentlichkeit vorgestellt. Das in Österreich entwickelte Produkt ist einzigartig und schließt eine zentrale Lücke im Angebot von Sicherheitslösungen. Im Kontext einer stark wachsenden Security Engineering Branche adressiert THREATGET die Zielgruppe der Fahrzeughersteller sowie aller Unternehmen, die Fahrzeugarchitekturen und -systeme analysieren, um Zertifikate vergeben zu können (z.B. der TÜV) sowie Personen im KFZ-Ausbildungsumfeld.

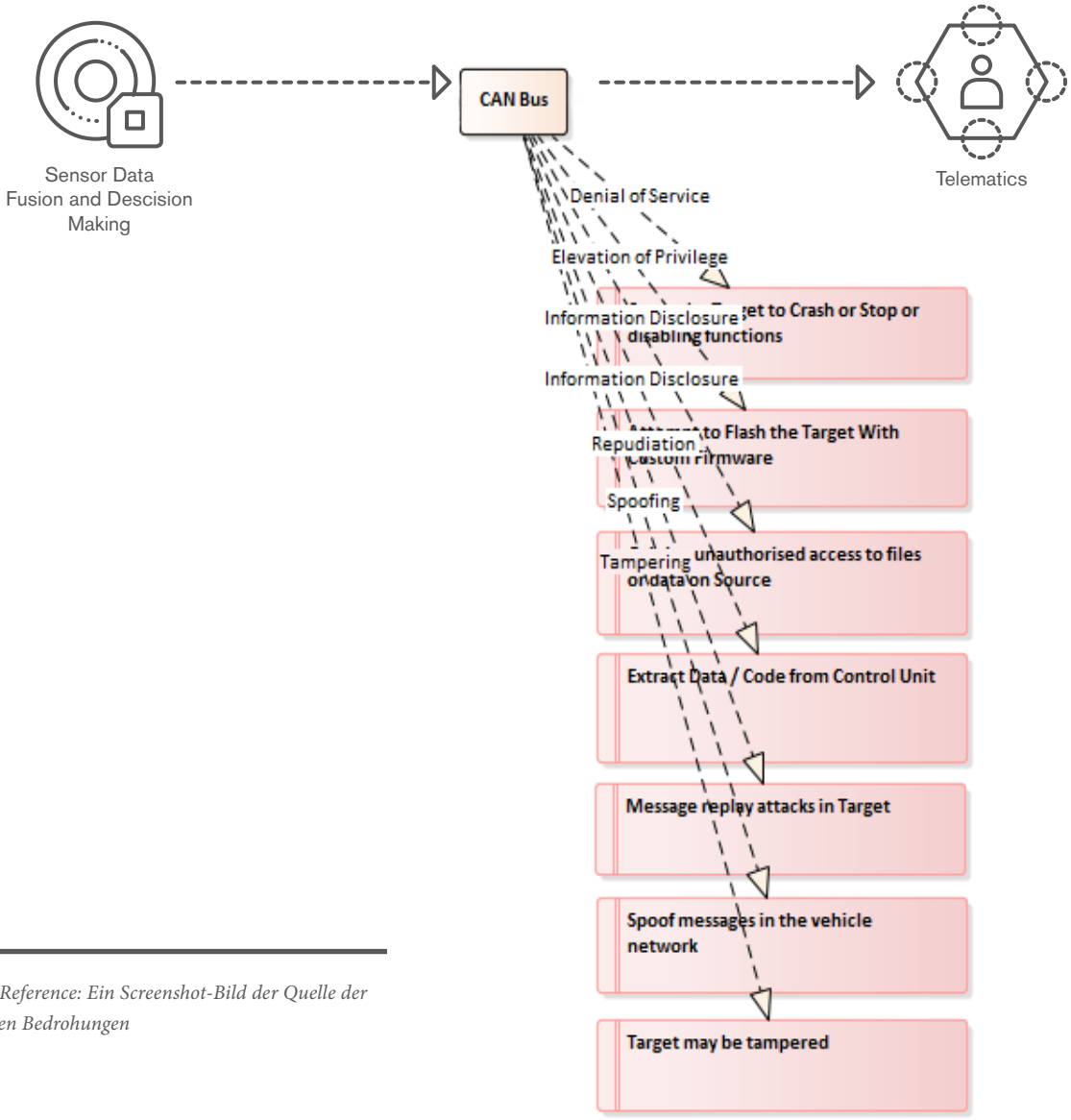
ARTIFICIAL INTELLIGENCE ZUR BEHERRSCHUNG VON KOMPLEXITÄT

Die in THREATGET enthaltene Datenbank mit Bedrohungspotential und Lösungsvorschlägen wird derzeit im Rahmen angewandter Forschung und Entwicklung gepflegt und gewartet. Anwender erhalten für das gewünschte Systemmodell (z.B. Fahrzeugplattform) eine Liste möglicher Probleme und daran geknüpfte Lösungsansätze, die dann von einem Security Engineer umgesetzt werden. In diesen manuell gewarteten Katalog fließen auch Updates weiterer Bedrohungskataloge ein, die z.B. von sogenannten Computer Emergency Response Teams (CERT) zusätzlich zusammengestellt werden. Mithilfe von Algorithmen, die sich Künstlicher Intelligenz (AI) bedienen, soll künftig das Update des THREATGET Katalogs um diese externen Bedrohungskataloge automatisch erfolgen. AI hilft auf diese Weise künftig dabei, die Komplexität der immer weiter steigenden Vernetzung unserer Systeme beherrschbar zu halten. THREATGET macht es möglich, dass künftig für alle Hersteller dasselbe Grundsicherheitsprinzip gewährleistet wird.

Darüber hinaus soll es für Hersteller von Spezialfahrzeugen (z.B. für den Sicherheitsbereich) auch möglich sein, auf diesem Grundsicherheitsprinzip aufzusetzen und gleichzeitig bestimmte Sicherheitslevel und -regeln in ihren Fahrzeugsystemen manuell zu erweitern. Der Markt für Lösungen im Bereich Cybersicherheit ist weltweit stark im Wachsen, da einerseits nun endlich gesetzliche Regelungen verbindlich werden und andererseits die Anziehungskraft für kriminelle Angriffe wächst. Europa positioniert sich dabei im Gegensatz zu anderen Ländern sehr klar als sicherheitsbewusster Markt. „Die Rahmenbedingungen in der EU für unsere Lösung sind sehr gut. Daher wollen wir den Markt nun rasch über unser Angebot informieren und den erarbeiteten Wissensvorsprung nutzen“, erklärt Lieber abschließend.

Helmut Leopold (links) und Peter Lieber (rechts) *freuen sich über die Markteinführung ihres gemeinsamen Produkts THREATGET.*

THREATS REFERENCE



Threats Reference: Ein Screenshot-Bild der Quelle der erkannten Bedrohungen

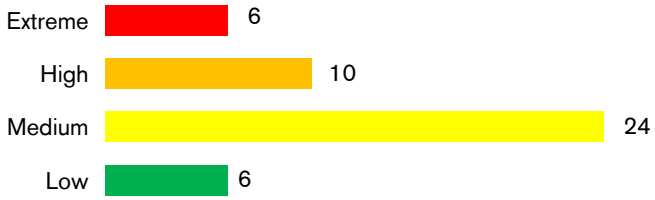
THREATS LIST

	Title	Type	Description	Impact	Likelihood
	16 Spoof me...	Spoofing	Forge or manipulate c...	Major	Likely
▶	17 Spoofing ...	Spoofing	Sensor Control Unit T...	Moder...	Possible
	18 Message ...	Repudiation	Packets or messages...	Major	Likely
	19 Gaining u...	InformationD...	Confidentiality of data...	Moder...	Possible
	20 Extract D...	InformationD...	Accessing data store...	Trivial	Remote
	21 Cause the...	DenialofSer...	DoS on Telematics C...	Critical	Certain

46 Threats Cyber Security Risk Assessment Risk Evaluation

Threats List: Details zu allen erkannten potenziellen Bedrohungen

THREAT SEVERITY



Threat Severity: Bewertet die Gefährlichkeit der erkannten Bedrohungen, um auf Grundlage der Parameter sowohl die Auswirkung als auch die Wahrscheinlichkeit zu ermitteln.

CYBER SECURITY RISK ASSESSMENT

		LIKELIHOOD					
		1 Remote	2 Unlikely	3 Possible	4 Likely	5 Certain	
IMPACT	1 Trivial	1	2	3	4	5	Low 1:5
	2 Minor	2	4	6	8	10	Medium 6:10
	3 Moderate	3	6	9	12	15	High 11:16
	4 Major	4	8	12	16	20	Extreme 17:25
	5 Crirtical	5	10	15	20	25	

Risk = Threat * Vulnerability * Consequence

Threat * Vulnerability = Likelihood

Consequence = Impact

THREATGET führt eine Risikobewertung durch, um das Risikoniveau aller erkannten Bedrohungen zu berechnen. Diese Risikostufen können über die THREATGET-Risikomatrix zugeordnet werden.

KONTAKT

LieberLieber
cybersecurity.lieberlieber.com

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY