hoch3 FORSCHEN

Das Medium für Wissenschaft

Herbst 2016

TECHNISCHE UNIVERSITÄT DARMSTADT

Impressum

Herausgeber
Der Präsident
der TU Darmstadt

Redaktion Stabsstelle
Kommunikation und Medien
der TU Darmstadt:
Jörg Feuck (Leitung, V.i.S.d.P.)
Ulrike Albrecht (Grafik Design)
Patrick Bal (Bildredaktion)

Gestalterische Konzeption
conclouso GmbH & Co. KG, Mainz

Titelbild Katrin Binner

Druck Frotscher Druck GmbH,
Darmstadt
gedruckt auf 100 g/m²
PlanoScript, FSC-zertifiziert

Auflage 5.700 **Nächste Ausgabe**
15. Dezember 2016

Leserservice presse@pvw.
tu-darmstadt.de

ISSN 2196-1506

Möchten Sie die nächste Ausgabe der hoch³FORSCHEN gerne in digitaler Form erhalten? Dann senden Sie bitte eine E-Mail an presse@tu-darmstadt.de

Der Weg zur Hirnsoftware

Menschen konstruieren aus ihrer Umgebung Sinn. Sie sammeln Eindrücke, hinterlegen diese als interne Repräsentationen im Gehirn und leiten daraus Verhalten ab. An der TU Darmstadt arbeiten Wissenschaftler daran, dass Computer bald ähnlich agieren können.

Von Hildegard Kaulen

Professor Constantin Rothkopf vom Zentrum für Cognitive Science der TU Darmstadt steht vor einer Herkulesaufgabe. Er will verstehen, wie Sehen und Handeln ineinandergreifen und wie diese Zyklen durch Algorithmen simuliert werden können. Dazu muss er begreifen, wie Nervenzellen Daten sammeln, kodieren und verrechnen und wie sie daraus Lösungen für anstehende Aufgaben ableiten. Weil technische Systeme in Zukunft vermehrt mit kognitiven Algorithmen ausgestattet sein werden, geht es Rothkopf um eine Software, die ein klein wenig so denkt und handelt wie ein Mensch.

Dazu bringt er die besten Voraussetzungen mit. Er ist Kognitionsforscher und Computerwissenschaftler, gehört zu den Gründungsmitgliedern des Zentrums für Cognitive Science und ist der erste Direktor. Hat das maschinelle Lernen seinem Feld nicht schon den Rang abgelaufen? „Maschinen erkennen zwar Sprache, Zahlen und Objekte sehr gut und neulich musste sich auch der Weltmeister im Go gegenüber einer Maschine geschlagen geben“, sagt Rothkopf. „Aber all diese Fortschritte erklären nicht, wie wir wahrnehmen, entscheiden und handeln. Wir verstehen den Zusammenhang zwischen den Lösungen der Maschinen und den Lösungen der Menschen nicht. Wenn es uns also um eine Hirnsoftware geht, müssen wir verstehen, wie das Gehirn die nötigen Datenmengen verarbeitet“, so Rothkopf weiter. „Dabei hilft uns das maschinelle Lernen zwar weiter, aber weil dabei andere Lösungen gefunden werden können als die, die wir finden, brauchen wir die Kognitionswissenschaft.“

„Durch kognitionswissenschaftliche Forschung können wir neue intelligente Lösungen für schwierige Probleme finden und viel über uns selbst lernen.“

Wie kommt es, dass drei Pfund Gehirn jeden Supercomputer in den Schatten stellen? „Das Gehirn arbeitet mit unvollständigen Daten“, erklärt Rothkopf. „Es generalisiert. Wenn Kinder wissen, was eine Katze ist, erkennen sie jede Art von Katze, auch eine aus Plüsch oder eine auf dem Papier. Eine Maschine schafft das bisher kaum. Das Gehirn lernt außerdem selbst und korrigiert sich selbst. Maschinen arbeiten vergleichsweise einseitig.“

Rothkopf interessiert sich besonders für natürliches Verhalten, das immer mit Unsicherheiten behaftet ist. Planen unter Unsicherheiten ist deshalb einer seiner Schwerpunkte. Er lässt Probanden eine Scheibe Brot mit Erdnussbutter bestreichen. Von der Datenverarbeitung her ist das ein hochkomplizierter Prozess. Denn wie jede sequentielle Arbeit muss auch das Bestreichen der Brote geplant und erlernt werden. Man braucht einen Teller, ein Messer, Brot und Erdnussbutter. Alles muss geholt und auf den Tisch gestellt werden. Dann müssen die Dinge in der richtigen Reihenfolge geortet, ergriffen, in der rechten Weise benutzt und zurückgestellt werden „Ein solcher Prozess braucht Augenbewegungen, Aufmerksamkeit, ein Arbeitsgedächtnis, sensorische Eindrücke und eine Aktionskontrolle“, sagt Rothkopf. „Dahinter steckt viel Beobachtung und Informationsverarbeitung. Kinder können erst mit neun bis elf Jahren perfekt sequentiell planen.“

Weil sich Rothkopf besonders für die Zyklen aus Sehen und Handeln interessiert, verfolgt er die Augen- und Körperbewegungen der Probanden beim Bestreichen der Brote. „Das Sehen hilft ihnen dabei, Unsicherheiten zu reduzieren“, sagt er. Der Prozess wird von vielen schnellen Augenbewegungen begleitet. Menschen entscheiden durchschnittlich dreimal pro Sekunde, wohin sie schauen. „In einer kürzlich abgeschlossenen Studie konnten wir zeigen, dass unsere Probanden in kontrollierten Laborumgebungen die Regelmäßigkeiten in ihrer visuellen Umgebung optimal lernen und für das Planen ihrer Augenbewegungen ihre eigene visuelle Unsicherheit und ihre Handlungsunsicherheit mit einberechnen. Dabei fassen unsere Datenverarbeitungsmodelle die

Informationen

Psychologie der Informationsverarbeitung
Prof. Dr. Constantin Rothkopf
Telefon: 06151/16-23367
E-Mail: rothkopf@psychologie.tu-darmstadt.de
www.pip.tu-darmstadt.de

Abbildung: Jan-Christoph Hartung

Professor Constantin Rothkopf (li.) und David Hoppe diskutieren Simulationsergebnisse.

Verhaltensdaten nicht einfach empirisch zusammen, sondern leiten sie aus allgemeinen Prinzipien der Informationsverarbeitung ab. Es gibt also ein computationales Modell der menschlichen Informationsverarbeitung. Eine der großen Fragen ist nun, wie sich dies auf alltägliche Handlungen, etwa auf die Zubereitung eines Sandwichs übertragen lässt."

Bei der Informationsverarbeitung im Gehirn spielen auch das Lernen und die in Aussicht gestellte Belohnung eine Rolle. Als Beleg nennt Rothkopf den Marshmallow-Test. Bei diesem Test bittet man ein Kleinkind, ein auf dem Tisch liegendes Marshmallow solange nicht zu essen, bis der Instrukteur ein zweites geholt hat. Dann lässt man das Kind mit der Süßigkeit alleine. Jahrzehntelang wurde das Verhalten des Kindes als Ausdruck seiner Selbstkontrolle gewertet. Für Rothkopf ist es das Ergebnis einer Computation im Gehirn. Das Gehirn verrechnet alle Eindrücke, Erfahrungen und Wünsche, kalkuliert Unsicherheiten ein und trifft dann eine Entscheidung, die in dem Moment die Beste ist, die unter den gegebenen Umständen getroffen werden kann.

Rothkopf begründet dies mit neuen Ergebnissen von Kollegen der Universität Rochester. Demnach warten Kinder, die unmittelbar vor dem Test eine in Aussicht gestellte Belohnung erhalten haben, durchschnittlich viermal länger als Kinder, die kurz zuvor mit einer leeren Versprechung abgespeist worden sind. „Auf das zweite Marshmallow zu warten, macht für das Kind also nur dann Sinn, wenn es aus Erfahrung weiß, dass seine Chancen auf einen zweiten Leckerbissen groß sind", sagt Rothkopf. „Hat es diese Erfahrung nicht gemacht, ist es klug, die vor ihm liegende Süßigkeit zu essen." Was die Psychologie jahrzehntelang als Charaktereigenschaft interpretiert hat, ist für ihn eine rationale Reaktion auf die Verrechnung aller Informationen und Repräsentationen. Das zeigt sich auch, wenn Probanden Aufgaben lösen, nachdem sie zuvor mit großem Erfolg oder Misserfolg Computer gespielt haben. „Zwei Minuten euphorisierendes oder deprimierendes Spielen hat extreme Auswirkungen darauf, wie sich die Probanden danach verhalten. Die beobachteten Effekte sind um ein Mehrfaches größer als die Effekte, die traditionell den Persönlichkeitsunterschieden zugeschrieben werden", sagt Rothkopf.

Er geht sogar noch einen Schritt weiter und sieht auch in einigen psychischen Erkrankungen das Ergebnis einer Computation im Gehirn. „Kollegen an der ETH Zürich haben überzeugend modelliert, dass derjenige, der immer wieder erlebt, dass sich nichts in seinem Leben ändert, egal was er tut, bei der Computation zu dem Schluss kommen kann, dass alle weiteren Anstrengungen sinnlos sind. Diese gelernte Hilflosigkeit, eine Passivität, kann sich dann als Depression manifestieren."

Rothkopf erwartet einiges von der Kognitionswissenschaft: „Durch diese Forschung können wir nicht nur neue intelligente Lösungen für schwierige Probleme finden, sondern auch viel über uns selbst lernen. Es geht hier im Grunde auch um Selbstoffenbarung."

Die Autorin ist Wissenschaftsjournalistin und promovierte Biologin.

Publikation:
David Hoppe & Constantin A. Rothkopf: Learning rational temporal eye movement strategies, Proceedings of the National Academy of Sciences (PNAS) 2016
doi: 10.1073/pnas.1601305113
www.pnas.org/content/113/29/8332

Mit Big Data zum Fahrzeug 5.0

Data Mining birgt Chancen und Risiken – auch für die Automobilindustrie. Wie sie Betriebsdaten von Fahrzeugen zielgerichtet und transparent nutzen kann, erforscht ein interdisziplinäres Team der TU Darmstadt.

Expertendiskussion: Hermann Winner (li.) und Stephan Rinderknecht, Professoren für Maschinenbau.

Von Jutta Witte

Data Mining ist an sich nichts Neues und mit Blick auf seine aggressive Nutzung durch die amerikanische Digitalwirtschaft hierzulande durchaus umstritten. Potentiale eröffnet das massenhafte Sammeln von Daten und deren Analyse mittlerweile auch für die Optimierung und Weiterentwicklung von Fahrzeugen. Doch wie schöpft man die neuen technologischen Möglichkeiten aus, ohne dass Datenschutz, Internetsicherheit und die Interessen der Nutzer auf der Strecke bleiben?

Vor dieser Frage steht gegenwärtig die deutsche Automobilindustrie: „Sie muss aus ihrem traditionellen Geschäftsverständnis heraus evolutionär vorgehen, dies aber in einem revolutionären Umfeld“, so beschreibt Christian Beidl, Leiter des Fachgebiets Verbrennungskraftmaschinen und Fahrzeugantriebe an der TU Darmstadt, die Situation. Im Rahmen einer gemeinsamen Forschungsinitiative wollen Wissenschaftler aus dem Maschinenbau, der Informatik und aus den Human- und Wirtschaftswissenschaften dieses Spannungsfeld auflösen.

Sie wollen Betriebsdaten von Fahrzeugen nicht wahllos, sondern für klar definierte Forschungs- und Entwicklungszwecke nutzen. „Wir sagen vorher, welche Daten wir für welche Anwendung brauchen“, betont Projektkoordinator Professor Stephan Rinderknecht. Ziel ist es, auf diesem Wege nicht nur, ausgehend vom einzelnen Fahrzeug, die Eigenschaften der Gesamtflotte zu verbessern, sondern auch die Entwicklung vom regelbasierten zum wissensbasierten Fahrzeug voranzubringen, das auf Basis seiner eigenen Daten „lernt“ und sich selbst kontrolliert und optimiert.

„Das Multiplexing war die Schlüsselinnovation, die das heutige Breitband-Internet und das mobile Internet erst ermöglicht hat“, schwärmt Küppers. Sein Team vom Fachbereich Elektrotechnik und Informationstechnik hat diese Technologie entscheidend verbessert und damit einen „gigantischen Markt“ eröffnet, wie der Forscher sagt. Vor kurzem hat ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Verbundprojekt der Darmstädter mit drei Industrieunternehmen die Technik reif für Feldtests gemacht.

Bislang fokussiere sich die Forschungslandschaft noch nicht sehr stark auf die Verbindung von Big Data und Automobiltechnologie, berichtet Rinderknecht, Leiter des Fachgebiets Mechatronische Systeme im Maschinenbau. „Insofern ist unser Forschungsvorhaben national und auch international beispielgebend.“ Das Besondere des Darmstädter Ansatzes: Experten aus zehn Fachgebieten verknüpfen das Thema Big Data und die Entwicklung neuer Technologien von Anfang an mit Fragen des Datenschutzes, der Cybersecurity, so genannten Human Factors wie dem Schutz der Privatsphäre, veränderten Kundenerwartungen und ökonomischen Aspekten. „Für unser Konzept ist es wichtig, für Transparenz zu sorgen und damit für Vertrauen und Akzeptanz bei den Nutzern“, sagt Rinderknecht. Mit den drei Säulen Leichtbau, Antriebe und Effizienz sowie Autonomes Fahren nimmt der Forschungsverbund die Topthemen der Automobiltechnologie in den Fokus. „Anhand dieser Anwendungsbeispiele für Data Mining wollen wir exemplarisch verschiedene Querschnittsthemen bearbeiten, die mit Blick auf die digitale Transformation

Informationen

Fachbereich Maschinenbau
Prof. Dr.-Ing.
Stephan Rinderknecht
(Projektkoordinator)
Institut für Mechatronische Systeme im Maschinenbau
E-Mail: rinderknecht@ims.tu-darmstadt.de
Telefon: 06151/16-23250
Prof. Dr. rer. nat.
Hermann Winner
Fachgebiet Fahrzeugtechnik
Prof. Dr. techn. Christian Beidl
Institut für Verbrennungskraftmaschinen und Fahrzeugantriebe

relevant sind“, erklärt Hermann Winner, Leiter des Fachgebiets Fahrzeugtechnik.

Daten sammeln moderne Autos schon heute, zum Beispiel Lastprofile von Verbrennungsmotoren, die Aufschluss darüber geben, wie dieser genutzt wurde, und bestimmen, wann der nächste Ölservice fällig ist. Eine flächendeckende Auswertung des gesamten Nutzungsprofils ist bislang aber noch nicht möglich, Optimierungen basieren derzeit noch auf Referenzanwendungen. Die Experten der TU Darmstadt sind überzeugt, dass sich enorme Verbesserungspotenziale ergeben könnten, wenn die „Betriebsphase zur Weiterentwicklungsphase“ wird.

Ausgangspunkt ihrer Forschungen ist das Konzept des individuellen Fahrzeugs. Innerhalb der zulässigen Toleranzen werde es nie ein exakt gleiches Fahrzeug geben, das exakt gleich genutzt werde, erklärt Winner. Jedes Fahrzeug generiert also individuelle Daten und kann sie zur Speicherung an einen Server weitergeben. Die Informationen werden analysiert, um Aussagen für die gesamte Flotte treffen zu können. Verbesserungen, die hierauf basieren, greifen jedoch erst in der nächsten Fahrzeuggeneration. Mit Hilfe neuer Big Data-Technologien könnte ein Fahrzeug zukünftig seine Daten hingegen auch zur Selbstoptimierung einsetzen, an den Server und andere Fahrzeuge weitergeben und die auf dieser Basis entstehende kollektive Intelligenz nutzen.

„Für unser Konzept ist es wichtig, für Transparenz zu sorgen und damit für Vertrauen und Akzeptanz bei den Nutzern.“

„Das Fahrzeug generiert selbst Wissen und profitiert davon“, sagt Winner. Das ist auch deswegen entscheidend, weil Probleme nicht im Regelbetrieb auftauchen, sondern vor allem bei dynamischen Vorgängen, zum Beispiel Bremsen und Beschleunigen auf nasser Fahrbahn oder auf steilen Straßen. Dann reagiert das Fahrzeug regelbasiert, das heißt, es gibt einen Kompromiss für jeden Betriebszustand. „Ein selbstlernendes Fahrzeug aber könnte ein jeweils optimales Fahrprofil generieren“, glaubt Christian Beidl. Auf der Basis zum Beispiel von Temperaturdaten und Lastzahlen passe ein solches Fahrzeug seine Betriebs- und Fahrstrategien unter Berücksichtigung bestimmter Ziele – weniger Emissionen oder geringe Bauteilbelastung – an.

Für Beidl ist dies mit Blick auf die Emissionen und die Umweltverträglichkeit der Fahrzeugantriebe ein nicht zu unterschätzender Vorteil. Heutige Abgasreinigungssysteme müssen regelbasiert für unterschiedlichste Fahr- und Umweltsituationen ausgelegt und dabei auch noch wirtschaftlich darstellbar sein. In diesem Zielkonflikt ist ein Optimum praktisch nicht erreichbar. Wenn jedoch ein intelligenter Betrieb das Optimum von Fall zu Fall selbst generiert, ist dieser Zielkonflikt auflösbar. So könnte beispiels-weise in immissionsbelasteten Innenstädten ein Betriebsmodus sichergestellt werden, mit dem eine weitere Belastung der Luftqualität verhindert wird. „Das bedeutet, wir erzielen bessere Ergebnisse für Menschen und Gesellschaft bei geringerem Ressourceneinsatz“, sagt der Experte.

Auch ein Blick auf den Leichtbau zeigt die neuen Möglichkeiten. So sind Getriebe in der Regel auf den extremsten Anwendungsfall ausgelegt. Man spricht dann vom „99-Prozent-Fahrer“. In Zukunft könnten Drehmomente und Temperaturprofile für Einzelereignisse wie hartes Schalten oder durchdrehende Räder erfasst werden und frühzeitig zeigen, wann Fahrzeugkomponenten ihre Nutzungsgrenze erreicht haben.

Daran anknüpfend wären völlig neue Geschäftsmodelle denkbar: Zugunsten einer leichteren und Ressourcen sparenderen Bauweise könnte das einmalige Auswechseln bestimmter Aggregate für den Fall extremer Nutzung von Anfang an in die Kalkulation einbezogen werden. Oder aber Menschen, die schonend mit ihrem Auto umgehen, könnten über ein Bonussystem belohnt werden. Es gäbe zudem präzisere Informationen, um Zustand und Wert eines Gebrauchtwagens zu bestimmen. Neue Prüfmethoden könnten entwickelt werden.

So deutet sich an vielen Stellen ein Paradigmenwechsel für die deutsche Automobilindustrie an. Die Forschungspartner wollen ihn wissenschaftlich vordenken. „Entscheidend ist“, hebt Rinderknecht hervor, „dass wir jetzt damit beginnen, die Daten zu sammeln, die wir für unsere Entwicklungsziele brauchen.“

Die Autorin ist Wissenschaftsjournalistin und promovierte Historikerin.

Forschungssäulen:
- Akzeptiertes autonomes Fahren
- Realfahrtoptimierte Antriebe
- Softwarebasierter Leichtbau

Querschnittsthemen:
- Big Data
- Human Factors
- Ökonomie und Ökologie
- Technische Methoden

bisherige Partner-Fachgebiete innerhalb der TU Darmstadt
- Arbeitswissenschaft & Systemgestaltung
- Fahrzeugtechnik
- Mechatronische Systeme im Maschinenbau
- Psychologie der Informationsverarbeitung
- Regelungsmethoden und Robotik
- Security Engineering
- Systemsicherheit
- Systemzuverlässigkeit, Adaptronik und Maschinenakustik
- Verbrennungskraftmaschinen und Fahrzeugantriebe
- Wirtschaftsinformatik, Software Business & Information Systems

Gehört zum Kernteam des Forschungsverbundes: Professor Christian Beidl (re.).

Abbildung: Katrin Binner

Lauschen verboten

Wenn zwei Menschen oder Software-Anwendungen im Web miteinander kommunizieren, liest manchmal ein Dritter heimlich mit. Kryptographische Verfahren könnten dies verhindern, aber Software-Entwickler tun sich mit der Umsetzung schwer. Deshalb wollen TU-Forscher die Verschlüsselung automatisieren.

Von Boris Hänßler

Andrea möchte ihrem Freund Stefan eine Nachricht schicken. Damit niemand mitliest, vereinbart sie mit Stefan mittels Kommunikation über das Netz einen geheimen Code, den nur er und sie entschlüsseln können. Falls die Nachricht in falsche Hände gerät, besteht sie ohne den Schlüssel nur aus einer unsinnigen Zeichenfolge. Was Andrea und Stefan allerdings nicht ahnen: Ein Spion hat sich dazwischen geschaltet. Der Code, auf den sich Andrea und Stefan geeinigt hatten, stammt in Wirklichkeit von diesem Spion. Er hat ihn den beiden Gesprächspartnern geschickt, indem er ihnen vorgaukelte, der jeweils andere zu sein. So kann er alle Nachrichten mitlesen und Andrea zum Beispiel um ein wichtiges Passwort bitten. Die fühlt sich sicher, weil sie denkt, sie schickt es ihrem Freund.

So ungefähr kann man sich eine Man-in-the-Middle-Attacke vorstellen, bei der ein Angreifer die Kommunikation im Internet manipuliert. Der Schlüssel oder Code, um den es geht, ist in der Informationstechnik Teil eines sogenannten kryptographischen Verfahrens. Es soll Daten schützen, die innerhalb einer Anwendung oder zwischen verschiedenen Anwendungen hin und her geschickt werden. Meist laufen Verschlüsselungsverfahren im Hintergrund ab, ohne dass wir sie als Nutzer bemerken. Wenn wir zum Beispiel einen Online-Shop besuchen, handeln unser Browser und der Online-Shop automatisch einen einzigartigen Schlüssel aus, mit dem die Daten, etwa die Bestellung oder Bankverbindung, mathematisch verfremdet werden. Ein Dritter könnte ohne Schlüssel nichts mit ihnen anfangen.

„Wissenschaftler aus der Kryptographie und Softwaretechnologie arbeiten hier eng zusammen. Das passiert weltweit noch viel zu selten."

Kryptographie begegnet uns ständig: Bei der Nutzung von Apps, beim Versenden von E-Mails, bei der Kommunikation über Messenger-Dienste oder bei der internen Kommunikation in Unternehmen – immer dann, wenn sensible Daten im Spiel sind. Verschlüsselungsverfahren gewähren eine gewisse Sicherheit unter bestimmten Annahmen hinsichtlich der Fähigkeiten der potentiellen Angreifer, aber nur, falls die Entwickler der Verschlüsselungsverfahren diese korrekt implementiert und die Entwickler der Anwendungen diese korrekt in ihren Code integriert haben. Und da liegen einige nicht vernachlässigbare Probleme: Die Einrichtung der Verfahren ist umständlich, und App- und Software-Entwickler sind keine Kryptographie-Experten. Sie machen Fehler. Allein in den Jahren 2013 bis 2015 sind 1769 Sicherheitsschwachstellen, die in der „National Vulnerability Database" (http://nvd.nist.gov), der nationalen Schwachstellen-Datenbank der USA, registriert wurden, auf solche Fehler zurückzuführen – damit waren in diesem Zeitraum Probleme mit der Integration von Verschlüsselungsverfahren in Anwendungen die vierthäufigste Quelle von registrierten Schwachstellen.

Das ist nicht verwunderlich, wenn man Studien betrachtet, die in den letzten Jahren während der wichtigsten wissenschaftlichen Konferenzen im Bereich der Cybersicherheit veröffentlicht wurden. Diese zeigen nämlich, dass die Integration eine wichtige Schwachstelle ist, insbesondere auch, weil die Nutzung kryptographischer Bibliotheken Wissen über zu viele Details erfordert, das Anwendungsprogrammierer oft nicht besitzen. Die Entwickler müssen etwa dafür sorgen, dass einzelne Schritte eines Verschlüsselungsverfahrens in einer bestimmten Reihenfolge ausgeführt werden. Dafür gibt es, je nachdem, was geschützt werden soll, konkrete Empfehlungen. Entwickler haben aber oft nicht die Zeit, sich mit entsprechenden Handbüchern zu beschäftigen. Eine weitere Fehlerquelle sind die sogenannten digitalen Zertifikate, welche die Gültigkeit eines Schlüssels bestätigen. Manchmal schalten Entwickler das Validierungsverfahren für die Zertifikate ihrer Software aus, um sie schneller testen zu können und vergessen anschließend, es wieder einzuschalten. „Beide Fehler geschehen häufig, auch bei seriösen Anbietern, und das sind nur zwei Beispiele unter vielen", sagt Mira Mezini, Leiterin des Fachgebietes Softwaretechnik an der TU Darmstadt. Angreifer haben stets den Vorteil, dass sie nur eine Sicherheitslücke finden müssen, um Daten abzugreifen, während die Entwickler vor der gewaltigen Aufgabe stehen, alle denkbaren Lücken zu schließen.

Es sei weder möglich noch sinnvoll, dass alle Software-Entwickler zugleich Verschlüsselungsexperten seien, insbesondere, wenn man bedenke, dass laut einem Bericht von IDC vom Dezember 2013, zu finden unter http://bit.ly/2a86Mju, unter den weltweit 18.5 Millionen Software-Entwicklern 7.5 Millionen Hobby-Programmierer seien – Tendenz steigend, so Mira Mezini. „Deshalb sollten sich Kryptographie-Experten und Software-Entwickler besser gegenseitig ergänzen." Genau das ist der Ansatz in dem von der Deutschen Forschungsgemeinschaft geförderten Sonderforschungsbereich „CROSSING" an der TU Darmstadt. Ein interdisziplinäres Team der TU Darmstadt entwickelt darin nicht nur neuartige Verschlüsselungsverfahren, sondern auch neuartige Sicherheitslösungen, um die Integration von Verschlüsselungsverfahren in Anwendungsprogrammcodes zu vereinfachen und damit langfristig das Vertrauen in die Informationstechnik zu stärken.

In „CROSSING" gibt es drei Schwerpunkte: Zum einen entwickeln die Forscher neue kryptographische Primitive. Das sind die kleinsten Bausteine in kryptographischen Verfahren. Im zweiten Schwerpunkt

Informationen

Fachgebiet Softwaretechnik
Prof. Dr.-Ing. Mira Mezini
Telefon: 06151/16-21360
E-Mail:
mezini@st.informatik.tu-darmstadt.de
www.stg.tu-darmstadt.de

entstehen aus diesen Primitiven neue kryptographische Systeme. Im dritten Schwerpunkt, in dem Mira Mezini beteiligt ist, unterstützen die Forscher die Software-Entwickler dabei, kryptographische Primitive und Systeme in ihren Anwendungen fehlerfrei einzusetzen. Gerade dies kam in der Cybersicherheitsforschung bisher zu kurz. „Bislang hat sie sich, wenn überhaupt, auf Endnutzer von Software konzentriert, um ihnen Software-Werkzeuge zur Verfügung zu stellen, mit denen sie sich vor schadhafter Software schützen können“, sagt Mezini. In CROSSING stünden erstmalig Software-Entwickler im Mittelpunkt.

Doch wie können die Forscher den Entwicklern helfen? „Unsere Annahme ist, dass die Fehler, die sie bei der korrekten Nutzung der kryptographischen Verfahren machen, deutlich reduziert werden können, wenn wir mehr auf die Bedürfnisse der Entwickler eingehen und sie aktiv bei der Integration der Verschlüsselungsverfahren in die Anwendungsprogrammcodes mit intelligenten Werkzeugen unterstützen, sprich mit intelligenten Verschlüsselungsbibliotheken, deren Komponenten zu einem signifikanten Anteil sich selbst automatisiert in die Anwendungscodes einbauen.“ In einem ersten Schritt hat Mezinis Team die Kernfrage in einer empirischen Studie an die Entwickler selbst gerichtet. „Entwickler arbeiten aufgabenorientiert“, sagt sie. „Sie wünschen sich Verschlüsselungsbibliotheken, die ihnen sagen: Diese Verschlüsselungskomponenten gibt es für deine Aufgabe, und so muss man sie konfigurieren, kombinieren und nutzen, damit sie für diese Aufgabe Sicherheit gewährleisten. Am besten wäre es, wenn die Bibliothek diese Aufgaben für die Entwickler übernehmen – also automatisiert umsetzen – könnte.“ Ein Entwickler möchte zum Beispiel einen Kommunikationskanal verschlüsseln. Die Bibliothek schlägt ihm dann die Komponenten für die Verschlüsselung vor und wie sie konfiguriert und integriert werden, damit sie sich gegenseitig nicht negativ beeinflussen. Das Ziel ist, geeignete softwaretechnische Methoden und Verfahren zu entwickeln, welche in intelligente Verschlüsselungsbibliotheken eingebaut werden. In einem weiteren Schritt soll das Verfahren weiter automatisiert werden. Am Ende gibt es in der intelligenten Verschlüsselungsbibliothek zwei Schnittstellen: Die eine besteht zu den Herstellern neuer kryptographischer Verfahren und überprüft, ob die Verfahren korrekt implementiert sind, die zweite zu den Software-Entwicklern und stellt sicher, dass korrekt implementierte Verschlüsselungsverfahren auch korrekt in Anwendungssoftware integriert und benutzt werden. So werden Verfahren doppelt geprüft – beim Hochladen in die Verschlüsselungsbibliothek und während der Implementierung der Anwendungssoftware. Letzteres geschieht idealerweise direkt in einer Software-Entwicklungsumgebung.

Software wird heute in solchen Entwicklungsumgebungen programmiert. Es handelt sich um integrierte Werkzeuge, die das Programmieren, Überprüfen und Testen von Software vereinfachen. Die populärste Entwicklungsumgebung für die Programmiersprache JAVA ist „Eclipse“. Mezini sagt: „Wir möchten zunächst die Funktionalität von Eclipse durch die Anbindung zu unserer intelligenten Verschlüsselungsbibliothek so erweitern, dass bereits während der Programmierung im Hintergrund laufend geprüft wird, ob die kryptographischen Algorithmen an der richtigen Stelle sind und korrekt konfiguriert und eingesetzt werden. Weitere Entwicklungsumgebungen können ebenso erweitert werden.“ Dieses Vorgehen würde zudem gewährleisten, dass eine Anwendung auch dann noch sicher bleibt, wenn der Programmierer sie weiter entwickelt bzw. wenn Verschlüsselungsverfahren, die über die Bibliothek integriert wurden, als nicht mehr sicher gelten. Die Entwickler sparen somit Zeit und können sich darauf verlassen, stets das aktuell bestmöglichste Verfahren eingesetzt zu haben.

Abbildung: Katrin Binner

Informatik-Professorin Mira Mezini, Leiterin des Fachgebiets Softwaretechnik an der TU Darmstadt.

Neben Mezini und dem Kollegen Eric Bodden, der vor einigen Monaten an die Universität Paderborn gewechselt ist, arbeiten zwei Doktoranden und ein PostDoc an dem Projekt. „Wir hoffen, dass langfristig eine aktive Community entsteht, die unsere Verschlüsselungsbibliothek lebendig hält“, sagt Mezini. „Eine wichtige Basis haben wir geschaffen, indem wir Kryptographen und Software-Ingenieure zumindest an der TU Darmstadt enger zusammen gebracht haben. Das passiert weltweit noch viel zu selten.“

Der Autor ist Technikjournalist.

Der neue Transsonik-verdichterprüfstand vor seiner Endmontage

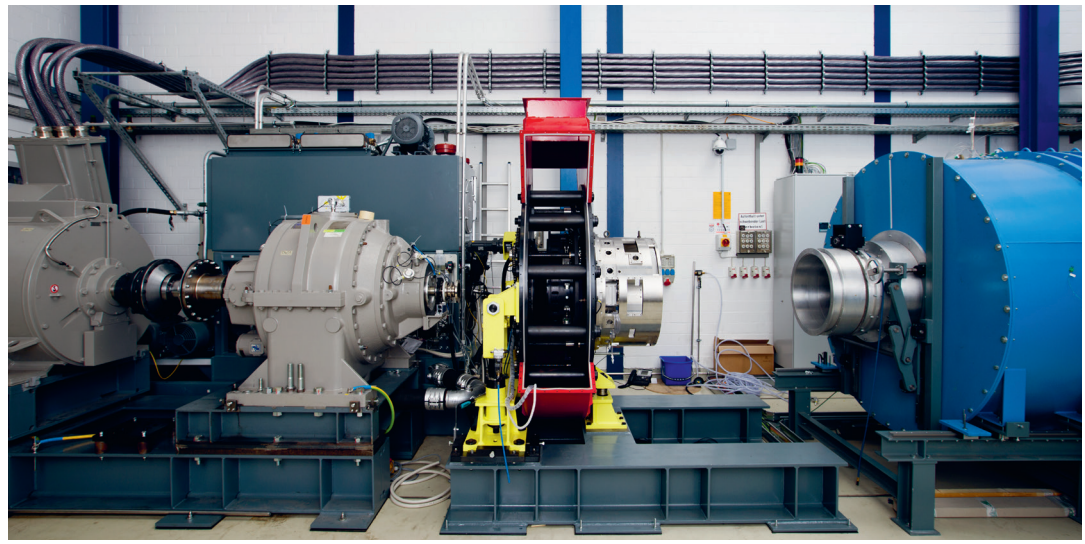

Abbildung: Katrin Binner

Turbokräfte

An der Technischen Universität Darmstadt entsteht ein leistungsstarker Prüfstand für Verdichter. Damit sollen Gasturbinen für die Energiewende fit gemacht werden.

Von Boris Hänßler

Ein Rohr mit dem Durchmesser eines Autoreifens führt von der Decke zum Boden, macht eine Wende und mündet in einer Reihe von Elementen, die an ein Flugzeugtriebwerk erinnern. Die Maschine im Verdichter-Prüfstand der TU Darmstadt saugt mit einer schnell drehenden Rotorbeschaufelung Luft von außerhalb des Gebäudes an und verdichtet sie. Dabei erreicht die Luft in manchen Bereichen Schallgeschwindigkeit. Stünde in dem Raum tatsächlich ein Triebwerk, würde der Verdichter die Luft mit etwa 20 Rotoren Stufe um Stufe von 1,5 bar auf 60 bar zusammen pressen. Zum Vergleich: Der Druck im Autoreifen beträgt zwei bis drei bar.

Die Forscher interessieren sich jedoch nur für die ersten Rotor-Stufen des Verdichters. „Sie sind die interessantesten“, sagt Professor Heinz-Peter Schiffer, Leiter des Fachgebiets für Gasturbinen, Luft- und Raumfahrtantriebe „In den Eingangsstufen werden die höchsten Geschwindigkeiten erreicht. Dort ist am meisten zu holen, wenn es um die Optimierung geht.“ Gasturbinen hätten heute zwar bereits hohe Wirkungsgrade, aber bei den hohen Energie-Mengen, die umgesetzt werden, bieten schon kleine Verbesserungen enormes Einsparpotential.

Schon seit 1994 betreibt die TU einen transsonischen Verdichter-Prüfstand, in dem Firmen wie MTU und Rolls Royce Verdichter von Flugzeugturbinen testen. Vor acht Jahren traf Schiffer die Entscheidung, einen zweiten Prüfstand einzurichten, um die Verdichterforschung auf Gasturbinen auszuweiten. Gasturbinen funktionieren ähnlich wie Flugzeugtriebwerke, sind aber größer und generieren an Stelle einer Schubkraft Wellenleistung. Der neue Prüfstand, der Ende des Jahres fertig sein wird, setzt deshalb mehr als doppelt so viel Leistung um wie der alte, und im Gegensatz zu diesem können die Forscher zukünftig auch zwei Stufen eines Verdichters testen statt nur eine – und damit auch die Wechselwirkungen zwischen den Stufen.

Der Verdichter im Prüfstand ist eine verkleinerte Version der Originale in Gasturbinenanlagen, aber die aerodynamischen Profile sind ähnlich und Druckverhältnisse identisch. „Es ist die kleinste mögliche Version, die noch realen Bedingungen entspricht“, sagt Schiffer. Nur unter realen Strömungsbedingungen können die Forscher den Betrieb in sicherheitskritischen Bereichen erforschen, etwa kurz vor dem Strömungsabriss oder der Beschädigung der Schaufeln. Weil solche Schäden die Gasturbine lahmlegen würden, gehen Ingenieure in der Praxis kein Risiko ein und nutzen nicht die Leistung, die theoretisch möglich wäre. Aber damit verschenken sie Potential. Je mehr sie die Verdichter ausreizen, desto effizienter wird die Gesamtmaschine. „In Darmstadt versprechen wir uns nun Messdaten, mit denen wir unsere Auslegungstools weiter kalibrieren können“, sagt Christoph Biela von Siemens, dem Kooperationspartner des neuen Prüfstands.

Die Instrumentierung ist in Darmstadt in der Tat einzigartig. Es gibt sogar auf den Rotoren Sensoren, mit denen die Schaufeln und ihre Schwingungen überwacht werden. „Im Prüfstand untersuchen wir die Strömungsfelder bei Eintritt, Austritt und in allen Zwischenstufen sowie den Wirkungsgrad in allen Betriebszuständen“, sagt Schiffer. Das mache den Prüfstand in der Zeit der Energiewende so wertvoll. Gasturbinen laufen derzeit meist mit konstanter Leistung. Um künftig auf Lastspitzen im Stromnetz flexibel reagieren zu können, müssen sie dynamisch betrieben werden. Ein schnelles Hoch- und Runterschalten hat allerdings Auswirkungen auf den Wirkungsgrad, die bisher nicht bekannt sind.

Die TU hat neben den Verdichter-Prüfständen übrigens auch zwei Turbinen-Prüfstände und ist damit im Turbomaschinenbau derzeit eines der weltweit führenden Institute.

Der Autor ist Technikjournalist.

Informationen

Institut für Gasturbinen, Luft- und Raumfahrtantriebe
Christian Kunkel
Telefon: 06151/16-22113
E-Mail:
kunkel@glr.tu-darmstadt.de