Saarland Informatics Campus SIC

Journalistenreise der Wissenschafts-Pressekonferenz

zum Saarland Informatics Campus vom 19. bis 21. Januar 2020

MONTAG, 20.01.2020

9:30 Uhr bis 12:15 Uhr
(DFKI, Geb. D3 3)

Deutsches Forschungszentrum für Künstliche Intelligenz – DFKI

Überblicks-Vortrag von Reinhard Karger, Unternehmenssprecher

Das Deutsche Forschungszentrum für Künstliche Intelligenz GmbH (DFKI) ist auf dem Gebiet innovativer Softwaretechnologien auf der Basis von Methoden der Künstlichen Intelligenz die führende wirtschaftsnahe Forschungseinrichtung Deutschlands. 1988 als gemeinnützige Public-Private-Partnership (PPP) gegründet, unterhält es Standorte in Kaiserslautern, Saarbrücken, Bremen, ein Projektbüro in Berlin, ein Labor in Niedersachsen und eine Außenstelle in St. Wendel. DFKI-Projekte adressieren das gesamte Spektrum von der anwendungsorientierten Grundlagenforschung bis zur markt- und kundenorientierten Entwicklung von Produktfunktionen. Am DFKI Saarbrücken findet Forschung an innovativen Software-Lösungen in den Bereichen Agenten und Simulierte Realität, Kognitive Assistenzsysteme, Multilinguale Technologien, Wirtschaftsinformatik, Smart Service Engineering und Algorithmic Business and Production statt.

Projekt Fühler im Netz 2.0 – KI für die Energiewende

Im Zuge der Energiewende werden viele kleinere Energieanlagen Großkraftwerke ersetzen und ihren Strom dezentral in das Netz einspeisen. Durch erneuerbare Energien kommt es zu Schwankungen. Das Projekt „Fühler im Netz 2.0“ will mittels Breitband-Powerline Technologie Kabel und Anlagen in Echtzeit überwachen. Über 3.500 Sensormodems werden dazu installiert, mit Machine Learning- und Deep Learning-Ansätzen werden die Daten auf Muster und Auffälligkeiten untersucht. Die Algorithmen erkennen Anomalien, lernen daraus und leiten so Vorhersagen oder eigene Strategien ab. Dies ist wesentlich für die Integration von E-Mobilität in die Verteilnetze.

Digital Reality zur synthetischen Erzeugung von Trainingsdaten

Professor Tim Dahmen, Head of Research Team Computational 3D-Imaging

Das Digital Reality-Konzept ist ein strukturierter Ansatz zur synthetischen Erzeugung von Trainingsdaten. Die zentrale Idee ist die Simulation von Messwerten an Szenen, die durch modulare parametrische Modelle der realen Welt erzeugt werden. Durch die Untersuchung des durch diese Modelle definierten Parameterraums können Trainingsdaten wesentlich kontrollierter erzeugt werden als Daten, die aus realen Situationen gewonnen wurden. Tim Dahmen stellt das Digital Reality-Konzept vor und demonstriert dessen Potenzial in verschiedenen Anwendungsbereichen, darunter die Inspektion von Produktionsanlagen, das Autonome Fahren, Smart Grid und die Materialwissenschaft.

12:15 Uhr bis 13:30 Uhr
Mittagessen, Fußweg zum Informatik-Gebäude E1 7

13:30 Uhr bis 14:30 Uhr
(Informatik-Gebäude E1 7, Seminarraum 0 08)

Programmieren im Neuro-Zeitalter
Sven Apel, Professor für Softwaretechnik, Universität des Saarlandes
Die zentrale Rolle von Software in unserer modernen Welt stellt hohe Anforderungen an die Qualität, Korrektheit und Zuverlässigkeit von Software-Systemen. Die Fähigkeit, Programmcode zu verstehen, spielt eine Schlüsselrolle bei Programmierern, damit sie die genannten Anforderungen erfüllen können. Trotz erheblicher Fortschritte unterliegt die Forschung zum Programmverständnis einer grundlegende Einschränkung: Programmverständnis ist ein kognitiver Prozess, der nicht beobachtet werden kann. Es sei denn, man verwendet bildgebende Verfahren, wie sie aus der Medizin bekannt sind. In dem Vortrag wird Professor Sven Apel seine neuesten Erkenntnisse vorstellen, die mit diesen bildgebenden Verfahren gewonnen wurden.

14:30 Uhr bis 15:30 Uhr
(Informatik-Gebäude E1 7, Seminarraum 0.08)

Softwaresysteme sollen ihr Verhalten selbst erklären
Holger Hermanns, Informatik-Professor der Universität des Saarlandes
(Lehrstuhl für Verlässliche Systeme und Software)

Selbst Experten verstehen das Verhalten komplexer Softwaresysteme immer weniger. Dabei regeln diese inzwischen immer stärker unseren Alltag, sei es als intelligente Haussteuerung, im autonomen Fahrzeug oder in der industriellen Produktion. Wissenschaftler der Universität des Saarlandes, zweier Max-Planck-Institute und der Technischen Universität Dresden entwickeln Mechanismen, die nicht nur Experten, sondern auch Laien das Verhalten komplexer Softwaresysteme verständlich machen. Die Deutsche Forschungsgemeinschaft fördert diesen Transregio-Sonderforschungsbereich mit elf Millionen Euro.“

15:30 Uhr bis 16:00 Uhr
Kaffeepause

16:00 bis 17:00 Uhr
(Max-Planck-Institut für Informatik, Geb. E1 4)

Synthese versus Analyse: Was wir aus Deep Fakes lernen können und welche Möglichkeiten KI-basierte Bildsynthese und Analyse eröffnen“
Christian Theobalt, Leiter der Forschungsgruppe „Graphics, Vision & Video“ am Max-Planck-Institut für Informatik und Informatik-Professor an der Universität des Saarlandes

Wir beleuchten neueste Entwicklungen aus dem Bereich der lerngestützten Computergrafik und Bilderkennung am Beispiel eines unserer aktuellen Projekte: Wir zeigen nicht nur einen neuartigen Ansatz zur Erstellung künstlicher, fotorealistischer Videos, sondern auch, wie dieser uns hilft, solche „Fälschungen“ mit möglichst hoher Treffsicherheit zu erkennen. Es wird deutlich werden, dass das maschinelle Lernen im Bereich Visual Computing viele Lösungen anbietet, dass aber auch neue Herausforderungen hinsichtlich der IT-Sicherheit entstehen. Wir werden aufzeigen, dass die Reduktion solch neuer KI-basierter Visual Computing Verfahren auf „Deep Fakes“ viel zu kurz greift, und es viele wichtige und spannende Anwendungsfälle dieser Technologie gibt, die zum Staunen einladen und unserer Meinung nach in der Berichterstattung bisher zu kurz gekommen sind.

DIENSTAG, 21.01.2020

9:30 Uhr bis 10:15 Uhr
(Informatik-Gebäude E1 7)

Digitalisierung 3.0 oder: Wie man jedem (Big) Data System vertrauenswürdiges Handeln beibringt
Professor Jens Dittrich, Leiter der „Data Analytics Group", Universität des Saarlandes

Professor Jens Dittrich wird das Forschungsprojekt ChainifyDB vorstellen. Mit seinem Team untersucht Jens Dittrich, wie automatischer Handel und Datenaustausch zwischen Firmen und anderen Institutionen ermöglicht werden kann, ohne dass sich die Teilnehmer dafür vollständig vertrauen müssen. Für diese Technologie gibt es zahlreiche vielversprechende Anwendungsdomänen – vom Handel und der Finanzindustrie über die Medizin bis hin zur Industrieproduktion. Für seine dafür entwickelte Technologie hat der Wissenschaftler ein Patent angemeldet. Das System ist billiger, leistungsfähiger und sicherer als existierende „Permissioned Blockchain"-Systeme. Das Projekt wird im Rahmen eines Forschungsprogramms für IT-Sicherheit des Bundesministeriums für Bildung und Forschung (BMBF), genannt StartUpSecure, mit 900.000 Euro gefördert. Info: https://chainifydb.com/

10:30 Uhr bis ca. 13:30 Uhr
(Helmholtz-Zentrum für IT-Sicherheit, CISPA, Geb. E9 1)

Überblick über die Forschung am CISPA Helmholtz Center for Information Security
Vortrag von Professor Michael Backes

Im Anschluss (ca. 11:15 Uhr) Präsentation ausgewählter Forschungsexponate und anschließender Diskussion in Kleingruppen mit gemeinsamem Mittagsimbiss.

Präsentierte Forschungsthemen:

Sicherheit von Gesundheitsdaten

Präsentation des neu gegründeten HMSP (Helmholtz Medical Security and Privacy Research Center: https://hmsp.center/) sowie Einblicke in einige Forschungsaspekte. Weltweit erheben Wissenschaftler Patientendaten, um für die Volkskrankheiten wie Demenz, Schlaganfall oder Tumorerkrankungen neue Therapien zu entwickeln. Diese Daten stammen etwa aus Blutproben oder Röntgenbildern und werden als multimediale Inhalte aus verschiedenen Quellen zusammengeführt. Die Forscher stehen nun vor der Herausforderung, wie sie diesen biomedizinischen Datenschatz effizient auswerten können, und zwar ohne die Privatsphäre des Patienten zu verletzen. Die dafür notwendigen vertrauenswürdigen Verfahren wollen Wissenschaftler zweier Helmholtz-Zentren in Saarbrücken und Bonn gemeinsam entwickeln. Sie haben jetzt das „Helmholtz Medical Security and Privacy Research Center (HMSP)" ins Leben gerufen.

Frühwarnsystem für Massenangriffe auf kritische Infrastrukturen

Massenangriffe im Internet, so genannte „Distributed Denial of Service Attacks", werden immer häufiger von Kriminellen für gezielte Angriffe, auch auf kritische Infrastrukturen, genutzt, bei denen sie besonders gravierenden Schaden anrichten. Oft werden dabei Verstärkungsangriffe genutzt, um mittels übernommener Server einen bestimmten Dienst mit einer großen Menge an Datenpaketen zu überlasten. Professor Rossow und sein Team haben ein globales Sensor-Netzwerk installiert, mit dem sie bisher bereits mehr als 14.752.744 Angriffe dokumentieren konnten. Durch das Identifizieren verschiedener Phasen ließ sich hieraus ein Frühwarnsystem entwickeln. Über eine spezielle Fingerprinting-Methode sind sogar Hinweise auf die Identität der Angreifer möglich.

Beweisbare Sicherheit bei Spectre-Angriffen

Die Spectre-Attacken, basierend auf spekulativer Ausführung von Befehlen und Seitenkanälen, haben die Hardware- und Softwareindustrien überrascht, und ihre Konsequenzen werden noch auf Jahre hinaus zu spüren sein. Da das Problem nicht auf dem Hardwarelevel gelöst werden kann ohne dafür die Effizienzsteigerungen aufzugeben, die durch spekulative Ausführung gewonnen werden, sind Lösungen auf dem Softwarelevel notwendig. Wir werden erläutern, wie Schwachstellen gegen solche Attacken auf dem Softwarelevel automatisch erkannt und behoben werden können, so dass wir beweisbare Sicherheit erreichen.

Cyberphysical Security

Cyberphysische Systeme bestehen aus vernetzten eingebetteten Geräten, die physikalische Prozesse messen und steuern. Beispiele solcher Systeme sind Industrie-Kontrollsysteme, Drohnen und Autos. Solche Systeme sind neuen Herausforderungen in Bezug auf die Sicherheit ausgesetzt, zum Beispiel Angriffe, die das System beschädigen. Jedoch kann die physikalische Ebene auch zum Erkennen von Angriffen und Anomalitäten eingesetzt werden. Wir stellen aktuelle Forschung im Bereich industrieller Kontrollsysteme und drahtloser Sicherheit vor.

Weitere Kurzpräsentationen und Diskussionen zu den Bereichen Authentifizierung, Adversarial Learning sowie Zuverlässigem Maschinellen Lernen.

14:00 bis 15:00 Uhr
(Zentrum für Bioinformatik, Geb. E2 1)

Forschungsergebnisse aus der Bioinformatik: Früherkennung von Demenz
Andreas Keller, Zentrum für Bioinformatik

Professor Andreas Keller vom Zentrum für Bioinformatik an der Saar-Uni leitet für ein Jahr ein Forschungsprojekt an der US-amerikanischen Eliteuniversität Stanford im Silicon Valley. Ziel ist, auf Einzelzellebene besser zu verstehen, wie Krankheiten wie Alzheimer und Parkinson im menschlichen Körper entstehen. Dadurch sollen solche Volkskrankheiten früher erkannt und neue Therapien gefunden werden. Der Ansatz von Kellers Arbeitsgruppe besteht darin, im Blut vorkommende Moleküle, so genannte Biomarker, zu nutzen, um Demenzkrankheiten möglichst früh zu erkennen.

15:00 Uhr bis 16:00 Uhr
(Max-Planck-Institut für Informatik, Geb. E1 4)

Internet der Zukunft
Anja Feldmann, Direktorin für Internet-Architektur am Max-Planck-Institut für Informatik

Die Max-Planck-Direktorin Anja Feldmann erforscht unter anderem Engpässe in Computernetzwerken und sucht nach Möglichkeiten, wie diese behoben werden kann. Sie beschäftigt sich zudem mit alternativen Netzwerkstrukturen und der Wide-Area Data Analytics