CISPA
Center for IT-Security, Privacy and Accountability

CRISP
Center for Research in Security and Privacy

KASTEL

Die Kompetenz-zentren für IT-Sicherheits-forschung

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Impressum

Verantwortlich für die jeweiligen Inhalte:
CISPA – Center for IT-Security, Privacy and Accountability
Campus E9 1
66123 Saarbrücken
Deutschland
Tel: +49 681 302-71922
Fax: +49 681 302-71942
E-Mail: office@cispa.saarland
https://www.cispa.saarland

CRISP – Center for Research in Security and Privacy
Mornewegstraße 32
64293 Darmstadt
Tel: + 49 6151 16 27282
E-Mail: info@crisp-da.de
https://www.crisp-da.de

KASTEL – Institut für Theoretische Informatik
Am Fasanengarten 5
Geb. 50.34
D-76131 Karlsruhe
Tel.: + 49 721 608-44213
Fax: + 49 721 608-55022
E-Mail: crypto-info@iti.kit.edu
https://www.kastel.kit.edu
—
Redaktion:
Andrea Ruffing, CISPA
—
Bildnachweise:
Titel: Dan Kuta / photocase.de
Einzelnachweise an den Bildern
—
Design:
gabriele jakobi – design strategien
—
Stand: Februar 2017



Fotos: Oliver Dietze

Vorwort

Die Digitalisierung und die ihr zugrundeliegenden Informations- und Kommunikationstechnologien (IKT) sind von zentraler Bedeutung für Gesellschaft, Staat, Wirtschaft und Wissenschaft. Die Medien berichten regelmäßig über Cyberkriminalität, gestohlene Passwörter und Kundendaten, Angriffe auf IT-Infrastrukturen, Beeinflussung politischer Wahlen durch Cyberspionage und Social Bots sowie über massive Eingriffe in die Privatsphäre, z. B. in und durch Social Networks.

Zumindest gefühlt wird die digitale Welt immer unsicherer. Auch die Forschung und Entwicklung zur Cybersicherheit und zum Schutz der Privatsphäre stehen angesichts der Geschwindigkeit der allgemeinen Entwicklung in der IKT vor großen Herausforderungen. Grund hierfür ist einerseits die explosionsartige Digitalisierung aller Lebensbereiche. Alles Physische wird digitalisiert und mit allem vernetzt. Die physische und digitale Welt verschmelzen. Gerade regulatorisch wird in Deutschland und Europa sehr viel für eine Verbesserung der Cybersicherheit getan. Gleichzeitig hat die Forschung und Entwicklung bezüglich Technik in den vergangenen Jahren deutlich zugenommen.

Die anhaltende massive Diffusion von Informationstechnologie mit all ihren Schwachstellen und die vielen real stattfindenden Angriffe tragen dazu bei, dass der Bedarf an Cybersicherheitsforschung und -entwicklung steigt. Hier sind Forschung und Entwicklung in allen Technologiereifegraden gefordert, von der erkenntnisorientierten Grundlagenforschung über die angewandte Technologieforschung bis hin zur Erprobung und Einführung im Markt. Die Cybersicherheitsforschung muss die Sicherheit der IT-Systeme von morgen behandeln, sie muss sich aber in mindestens gleichem Maße um die Sicherheit der bereits vorhandenen Informationstechnologie kümmern.

Seit 2011 finanziert das Bundesministerium für Bildung und Forschung (BMBF) als zentralen Baustein der Digitalen Agenda die drei Kompetenzzentren für IT-Sicherheitsforschung CISPA (Saarbrücken), CRISP (Darmstadt) und KASTEL (Karlsruhe) und hat damit die dringend notwendige deutliche Vergrößerung der Forschungskapazitäten in Deutschland ermöglicht. Seit Beginn der Förderung durch das BMBF haben die drei Zentren sich zu international sichtbaren und renommierten Größen entwickelt, deren exzellente Forschung sich mit Einrichtungen von Weltrang messen kann. In Europa bereits unter den führenden Institutionen, tragen die Zentren mit ihren wichtigen internationalen Kooperationen, sowohl innerhalb Europas als auch außerhalb, zum dringend gebotenen globalen Austausch von Wissen und Talenten, und damit zur digitalen Souveränität Deutschlands und Europas bei.

In der Ihnen vorliegenden Broschüre möchten wir als Sprecher der drei BMBF-geförderten Kompetenzzentren für IT-Sicherheitsforschung Ihnen die Institute, deren Standorte und zentrale Forschungsprojekte vorstellen. Wir möchten die Chance nutzen und aufzeigen, in welchem Maße die Breite des von den drei Zentren gemeinsam abgedeckten Themenspektrums zu einer sicheren, souveränen und selbstbestimmten Zukunft beiträgt, sie sogar erst ermöglicht.

Wir wünschen Ihnen eine anregende Lektüre.

Prof. Dr. Michael Backes | Prof. Dr. Michael Waidner | Prof. Dr. Jörn Müller-Quade

CISPA Saarbrücken

Das Forschungszentrum für IT-Sicherheit an der Universität des Saarlandes

CISPA
Center for IT-Security, Privacy and Accountability

SAARBRÜCKEN: Das 2011 gegründete „Center for IT- Security, Privacy and Accountability“ (CISPA) ist das Forschungszentrum für IT-Sicherheit in Saarbrücken, das sowohl von der Universität des Saarlandes, als auch von den beiden Max-Planck-Instituten für Informatik (MPI-INF) und Softwaresysteme (MPI-SWS), sowie dem Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) unterstützt wird. Mehr als 415 WissenschaftlerInnen forschen am Standort Saarbrücken an IT-sicherheitsrelevanten Themen, 211 davon im Kernbereich des CISPA. Gemeinsam erarbeiten Sie für das CISPA anhand eines ganzheitlichen Ansatzes Lösungen für die Kernprobleme der IT-Sicherheit und des Datenschutzes in der Digitalen Gesellschaft. Das Zentrum kombiniert hierzu eine breite Grundlagenforschung zur Analyse bestehender und Entdeckung neuer Lösungsansätze mit deren systematischer Weiterentwicklung zu einem universellen Werkzeugkasten von praktisch einsetzbaren Sicherheitstechnologien in komplexen Gesamtsystemen.

Unter dem Motto „Sicherheit und Datenschutz für die digitale Gesellschaft“ werden wegweisende und grundlegende Techniken systematisch zu einsatzbereiten Sicherheitslösungen weiterentwickelt, die in Zusammenarbeit mit Partnern aus der Industrie, sowie eigenen Spin-Offs in vermarktbaren Produkten zum Einsatz kommen. Die Forschungsschwerpunkte orientieren sich vor allem an den beiden Leuchttürmen „Big Data Privacy“ und „Benutzbare Sicherheit für mobile Systeme“. Ein besonderes Augenmerk liegt auch auf den internationalen Kooperationen des CISPA – in der Großregion mit Luxemburg und Nancy, aber auch global mit der Eliteuniversität Stanford, USA, insbesondere seit der Gründung des CISPA-Stanford Center für Cybersicherheit im Oktober 2016.

CISPA – Center for IT-Security, Privacy and Accountability
Campus E9 1
66123 Saarbrücken
Deutschland
Tel: +49 681 302-71922
Fax: +49 681 302-71942
E-Mail: office@cispa.saarland
https://www.cispa.saarland

Foto: Christoph Sorge

Fast Facts

- 6 ERC-Grants, insbesondere ERC Synergy Grant „imPACT“
- „CISPA-Stanford Center for Cybersecurity“ als Basis exzellenter Grundlagenforschung
- DFG-Sonderforschungsbereich 1223 „Methoden und Instrumente zum Verständnis und zur Kontrolle von Datenschutz“
- Bachelor- und Masterstudiengang „Cybersicherheit“
- Über 210 WissenschaftlerInnen im Kernbereich des CISPA, 415 in IT-sicherheitsrelevanten Themen am Standort
- Gemeinsame Förderung durch das BMBF und die Staatskanzlei des Saarlandes
- Eingebettet in Informatikstandort von Weltrang

Leuchttürme

Big Data Privacy

Einer der wichtigsten Schwerpunkte des CISPA liegt auf anwendungsorientierter Forschung zu Privacy und Privacy-by-Design-Lösungen im Kontext von Big Data. Nicht zuletzt wurde dies auch durch den ERC-Synergy-Grant für Forschung in diesem Bereich belegt. Hierbei stellt unsere Forschungsarbeit den Endnutzer und die Wahrung seiner Interessen und Rechte in den Mittelpunkt. Mehrere Forschungsgruppen befassen sich schon seit 2011 mit den Grundlagen der Privatsphäre in der digitalen Gesellschaft. Vermehrt arbeitet CISPA seit 2015 nun auch stärker den Anwendungsbezug zum Internet der Dinge, insbesondere im Bereich Big Data, heraus. Die datenschutzbewahrende Aufbereitung, Verarbeitung und Analyse großer Datenmengen mit potenziellem Personenbezug wird ein Kernproblem künftiger Innovationen im Internet der Dinge und für die Industrie 4.0 sein. Insofern wird CISPA diesen Schwerpunkt auch weiterhin ausbauen.

Benutzbare Sicherheit für mobile Systeme

Foto: Oliver Dietze

In der ersten Förderphase hat CISPA bereits herausragende Forschungserfolge im Bereich der „Mobile Security“ erzielt, insbesondere hinsichtlich der Berechtigungen von Apps und der Sicherheit des Android-Betriebssystems für Endnutzer. Hierauf baut die aktuelle Forschung auf. Mit stärkerer Industrieorientierung forscht CISPA an einer Middleware mit Sicherheitsgarantien, um den Einsatz von Android in hochkritischen Bereichen in Firmen oder Regierungen zu ermöglichen. Des Weiteren zielt die Forschung darauf ab, die Benutzbarkeit von Sicherheitsfeatures für Endnutzer und Entwickler zu verbessern.

Foto: Oliver Dietze

Prof. Michael Backes

Foto: Manuela Meyer

Prof. Peter Druschel

Foto: Andreas Zeller

Prof. Andreas Zeller

Foto: Manuela Meyer

Prof. Christian Rossow

Weitere Forschungsschwerpunkte

Aus den vielfältigen Forschungsgebieten des CISPA lässt sich insbesondere eine schwerpunktmäßige und erfolgreiche Arbeit in folgenden ausgewählten Forschungsgebieten ablesen:

- Cryptography
- Information Retrieval and Machine Learning
- Programming Language Principles and Verification
- Societal and Legal Concepts
- Software Security
- System Design Principles
- Threat Analysis & Modeling
- Usable Privacy & Security

Sicherheit und Datenschutz für die digitale Gesellschaft

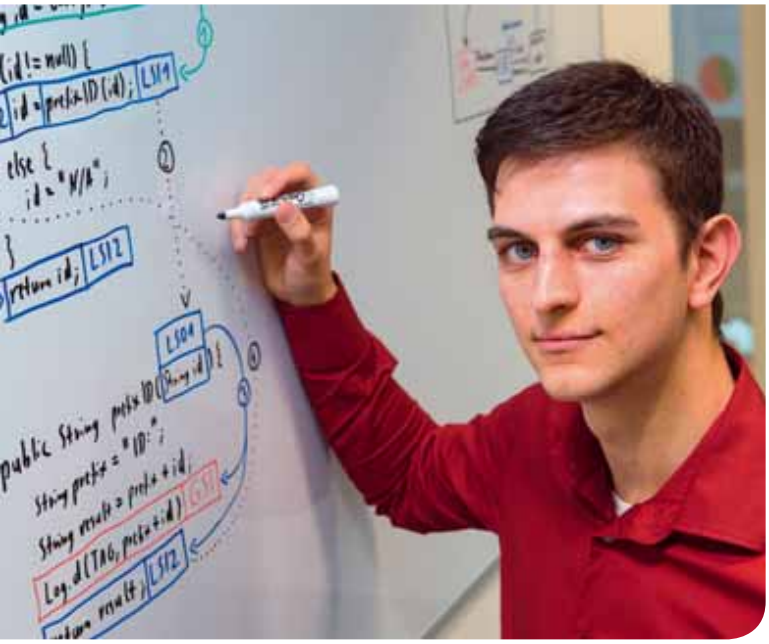


Foto: Oliver Dietze

Der Standort Saarbrücken

Als wissenschaftliche Einrichtung an der Universität des Saarlandes vereint das CISPA sämtliche IT-Sicherheits- und Datenschutzforschung auf dem Campus. CISPA hat mit seinen Kooperationspartnern, dem Max-Planck-Institut für Informatik, dem Max-Planck-Institut für Softwaresysteme, dem Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI), dem DFG-geförderten Exzellenzcluster „Multimodal Computing and Interaction“ und dem Fachbereich für Informatik der Universität des Saarlandes ideale Voraussetzungen um in dieser Umgebung umfassende und ganzheitliche IT-Sicherheitsforschung zu betreiben. Mit seinen lokalen sowie seinen französischen Partnern des „Laboratoire lorrain de recherche en informatique et ses applications“ (LORIA), in Nancy, Frankreich hat CISPA eine gemeinsame Forschungsagenda für IT-Sicherheit und Datenschutz entwickelt, die im Rahmen von sich ergänzenden Forschungsprojekten gemeinsam und strukturiert bearbeitet wird. Das seit 2011 vom Bundesministerium für Bildung und Forschung geförderte Kompetenzzentrum für IT-Sicherheitsforschung CISPA bildet dabei den Kern dieses Forschungsstandorts.

Sonderforschungsbereich 1223: „Methoden und Instrumente zum Verständnis und zur Kontrolle von Datenschutz“

Der 2016 errichtete Sonderforschungsbereich umfasst 19 Forscher, 27 Doktoranden und wird in Saarbrücken am CISPA koordiniert. Die beteiligten Institutionen sind grenzüberschreitend das DFKI, das Max-Planck-Institut für Informatik (MPI-INF), das Max-Planck-Institut für Softwaresysteme (MPI-SWS), das LORIA (Nancy) sowie die Universität Luxemburg.

ERC-Grants

Seit 2011 hat CISPA 6 ERC Grants erhalten, allen voran den mit 10 Mio. € dotierten Synergy Grant, der höchsten Auszeichnung und Forschungsförderung, die der Europäische Forschungsrat vergibt.

- ERC Synergy Grant „imPACT“(Michael Backes, Peter Druschel, Rupak Majumdar, Gerhard Weikum)
- ERC Advanced Grant „SPECMATE“(Andreas Zeller)
- ERC Consolidator Grant „OSARES“(Bernd Finkbeiner)
- ERC Consolidator Grant „RustBelt“(Derek Dreyer)
- ERC Starting Grant „NOLEPRO“ (Matthias Hein)
- ERC Starting Grant „iSkin“(Jürgen Steimle)

Foto: Oliver Dietze

Forschungsthemen

CISPA-Stanford Center

CISPA hat mit der US-amerikanischen Elite-Universität Stanford eine Forschungs- und Ausbildungskooperation für Cybersicherheit aufgebaut, deren Ziel vor allem darin besteht, exzellente Nachwuchskräfte auf dem Gebiet der IT-Sicherheit auszubilden, die zukünftig in Forschung und Industrie Führungsverantwortung übernehmen können. Mit diesem Forschungsprogramm des Zentrums, das sich an promovierte WissenschaftlerInnen und GruppenleiterInnen richtet, wurde ein europaweit einzigartiges Qualifikationsumfeld geschaffen, das die Stärken beider Standorte vereint. Teilnehmer des Programms verbringen zunächst 1-2 Jahre am CISPA, arbeiten danach 2 Jahre lang als Assistant Professor an der Universität Stanford, bevor sie wieder zurück ans CISPA kommen, um dort für 3 Jahre eine Nachwuchsgruppenleiterstelle anzutreten. Das Bundesministerium für Bildung und Forschung (BMBF) fördert diese Kooperation am CISPA umfassend. Vorbild für die Einrichtung ist das Max Planck Center for Visual Computing and Communication, das 2003 vom Max- Planck-Institut für Informatik und der Stanford University gegründet wurde und ebenfalls vom BMBF gefördert wird.

CISPA-Stanford Center
FOR CYBERSECURITY

Nachwuchs und Ausbildungsmöglichkeiten: Bachelorstudiengang „Cybersicherheit“

Seit dem Wintersemester 2014/15 bietet das CISPA mit seinen Partnerinstituten den neuen Bachelorstudiengang „Cybersicherheit” als Ergänzung zu den bisherigen Bachelorstudiengängen im Bereich der Informatik in Saarbrücken an. Somit können Studenten sich schon frühzeitig spezialisieren und einen idealen Grundstein für eine Karriere in der IT-Sicherheitsforschung legen. Bereits 2016 waren 230 Studenten für Cybersicherheit eingeschrieben. Vertiefend können Bachelorabsolventen den EIT ICT Masterstudiengang „Security & Privacy“ besuchen. In Zusammenarbeit mit der Graduiertenschule für Informatik bietet das CISPA Doktorandenstellen zur Verstärkung der mehr als 30 Forschungsgruppen des Zentrums an.

Foto: CISPA

Bürgerdialog: IT-Sicherheitsinitiative Saar

Die IT-Sicherheitsinitiative Saar ist ein Programm, das Anfang 2016 von CISPA als Mitgründer gestartet wurde und den Transfer von Forschungserkenntnissen, aber auch den Austausch zwischen Forschung und Industrie im Saarland zum Ziel hat. Hier werden Veranstaltungen im Rahmen einer Vortragsreihe angeboten und langfristig Treffen zwecks Erfahrungsaustauschs zwischen den Mitgliedern der Initiative angestrebt. Der Dialog mit Bürgern und der Transfer von Wissen sind auch zwei der Kernziele des Kompetenzzentrums CISPA.

CRISP Darmstadt

CRISP

Center for Research
in Security and Privacy

Fast Facts

- Allianz aus vier renommierten Forschungseinrichtungen am Standort Darmstadt
- Forschungsschwerpunkt „Security at Large“: Sicherheit großer komplexer Systeme
- Spektrum von der Grundlagenforschung bis zur Anwendung
- Über 450 WissenschaftlerInnen
- Mehrere DFG-geförderte Spitzenforschungsprojekte
- Masterstudiengang IT-Sicherheit und berufliche Weiterbildung
- Gemeinsame Förderung durch das BMBF und das HMWK

CRISP – Das Center for Research in Security and Privacy

Die Forschung in CRISP steht unter dem zentralen Thema „Security at Large“, der Sicherheit großer Systeme. Die Wissenschaftlerinnen und Wissenschaftler arbeiten nicht nur an der Sicherheit einzelner Komponenten, sondern darüber hinaus an deren Zusammenspiel in umfassenden Sicherheitslösungen.

Die Leuchtturmprojekte „Sichere Internet-Infrastrukturen“ und „Sichere Web-Anwendungen“ nehmen dabei einen herausgehobenen Stellenwert ein.

CRISP ist ein Zusammenschluss von vier renommierten Forschungseinrichtungen im Bereich Cybersicherheit: die Technische Universität Darmstadt mit ihrem Profilbereich für IT-Sicherheitsforschung CYSEC, die Hochschule Darmstadt, das Fraunhofer-Institut für Sichere Informationstechnologie SIT und das Fraunhofer-Institut für Graphische Datenverarbeitung IGD. Diese Partnerschaft ist die europaweit größte Allianz von Forschungseinrichtungen im Bereich Cybersicherheit.

Die Forschungsarbeiten in CRISP erfolgen interdisziplinär, sowohl in der Grundlagen- als auch in der anwendungsorientierten Forschung. So bringen auch Fachgebiete außerhalb der Informatik – zum Beispiel Physik, Maschinenbau oder Psychologie – ihre Expertise mit ein. Außerdem arbeitet CRISP in nationalen und internationalen Kooperationen mit zahlreichen Forschungseinrichtungen und Industriepartnern zusammen.

CRISP wird gefördert vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK). Die beiden Ministerien haben bis zur Gründung von CRISP im Jahr 2015 die beiden Darmstädter Sicherheitszentren EC SPRIDE bzw. CASED gefördert, die in CRISP aufgegangen sind.

CRISP – Center for Research in Security and Privacy
Mornewegstraße 32
64293 Darmstadt
Tel: + 49 6151 16 27282
Mail: info@crisp-da.de
https://www.crisp-da.de

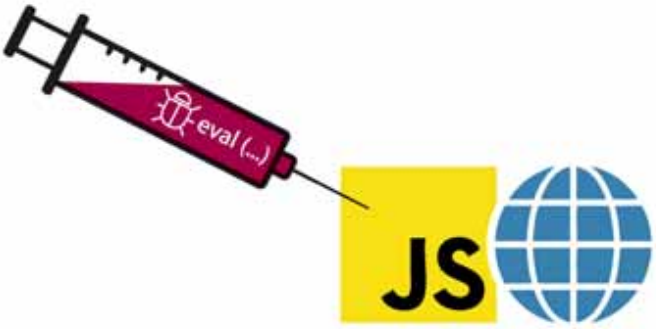
Leuchttürme

Sichere Internet-Infrastrukturen

Das Internet ist das größte und komplexeste Kommunikationsnetz und die weltweit größte IT-Infrastruktur. Zentral für das einwandfreie Funktionieren des Internets ist das Domain Name System (DNS) und entsprechende Protokolle wie z. B. das Border Gateway Protocol (BGP).
DNS- und BGP-Server bilden das Rückgrat des Internets und sorgen z.B. dafür, dass E-Mails sicher ihr Ziel erreichen, indem Daten den Weg entsprechend eigenständig wählen. Die Wegewahlfunktionen im Internet helfen dabei, auf unvorhergesehene Ereignisse wie etwa den Ausfall von Internet-Knoten zu reagieren und sichern so die Verfügbarkeit des Internets.
Doch die Wegewahl kann auch missbraucht werden, indem Datenpakete bewusst über bestimmte Internetknoten gelenkt werden, um somit auf Inhalte zugreifen zu können und diese auszulesen oder zu verändern.
Über Analyseverfahren gelang es, besonders gravierende Schwachpunkte in den Internet-Infrastrukturen zu identifizieren und das Ausmaß der Bedrohungen zu bestimmen. Demnach sind über 70 Prozent der getesteten DNS-Server in Unternehmensnetzen verwundbar. Das Leuchtturmprojekt „Sichere Internet-Infrastrukturen“ entwickelt hierzu Handlungsempfehlungen sowie neue Protokolle und Cybersicherheitslösungen, um den globalen Herausforderungen in diesem Bereich zu begegnen.

Sichere Web-Anwendungen

Die Sicherheit von Webanwendungen betrifft Millionen von Internetnutzern – immer mehr Menschen nutzen Onlinebanking, kaufen im Internet ein oder versenden E-Mails. Es ist bekannt, dass viele dieser Anwendungen unsicher sind.
Viele Softwareprogramme werden heute aus dem Internet geladen. Das bedeutet, sie müssen nicht mehr lokal installiert werden, sondern werden jeweils vor der Benutzung über das Internet in einen Webbrowser geladen und danach ausgeführt. Die Programmierung solcher Software erfolgt sehr häufig in der Programmiersprache JavaScript. Die Erfahrung zeigt jedoch, dass in JavaScript programmierte Anwendungen oftmals Schwachstellen enthalten.
Um die Sicherheit von Web-Anwendungen zu verbessern, werden im CRISP-Leuchtturmprojekt „Sichere



Web-Anwendungen“ Programmanalysen entwickelt, die Schwachstellen in mit JavaScript erstellter Software aufspüren, damit sie schnell behoben werden können. Hierzu braucht man Software, die möglichst effizient nach Sicherheitsrisiken sucht, insbesondere dann, wenn es sich um umfangreiche Softwareprogramme handelt.
Eine neuartige Kombination von Analysen bei der Ausführung dieser Software und Verfahren zu Generierung von Interaktionssequenzen ermöglicht es, das Verhalten solcher komplexer Internetanwendungen vollautomatisch zu analysieren und diese damit zuverlässiger und sicherer zu machen.

Darmstadt – ein renommierter Standort in der internationalen Cybersicherheitsforschung

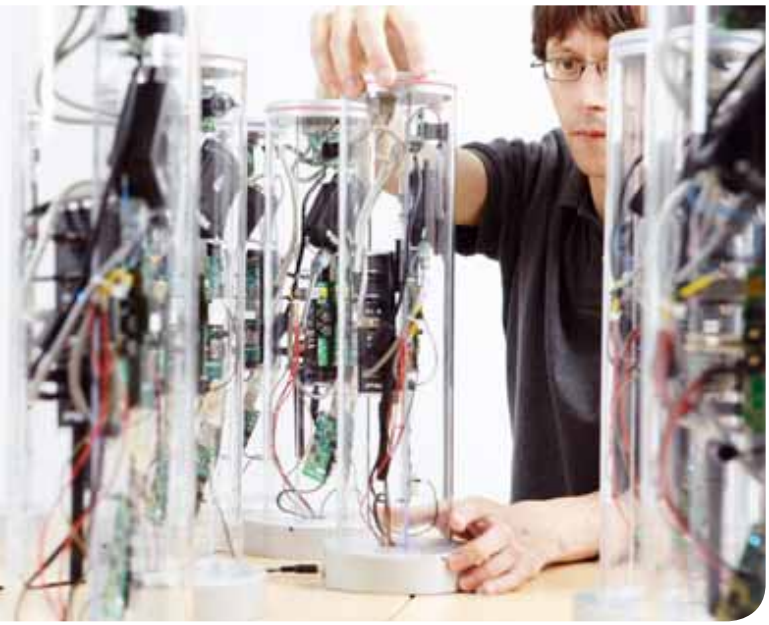


Foto: Katrin Binner

Darmstadt zählt heute zur internationalen Spitze in der Cybersicherheitsforschung und blickt auf eine lange Tradition von Cybersicherheitszentren zurück. Das Darmstädter Zentrum für IT-Sicherheit (DZI) wurde bereits 2002 als Allianz von TU Darmstadt, Fraunhofer SIT und Fraunhofer IGD gegründet. Seit 2008 wurde die Cybersicherheit am Standort Darmstadt durchgehend vom Land Hessen, seit 2011 auch vom Bund gefördert. Diese Investition zahlt sich aus: Mittlerweile arbeiten über 450 Wissenschaftlerinnen und Wissenschaftler in Darmstadt an aktuellen Themen der Cybersicherheitsforschung. Die Größe der Allianz bietet den Wissenschaftlerinnen und Wissenschaftlern ein thematisch vielfältiges Forschungsumfeld mit kurzen Wegen und leichtem Zugang zu einem großen internationalen Netzwerk. Die zentrale Lage im Rhein-Main-Gebiet mit der hervorragenden Anbindung an den internationalen Flughafen Frankfurt ist ein weiterer Standortvorteil.

Forschungsthemen

Forschungsfokus – Security at Large

CRISP richtet seine Forschung auf „Security at Large“ aus. Im Fokus stehen die Herausforderungen, die sehr große, integrierte Systeme mit sich bringen. Beispielsweise haben Softwaresysteme heutzutage eine enorme Komplexität. Schwachstellen in Softwaresystemen müssen frühzeitig entdeckt werden, damit Angreifer sie nicht ausnutzen können. Das nachträgliche Schließen der Lücken, in Form ständiger Updates für die Nutzerinnen und Nutzer, ist aus Sicht der IT-Sicherheit nicht die optimale Lösung. CRISP erarbeitet daher neue Analysemethoden, die helfen, solche Schwachstellen bereits in der Entwicklung zu identifizieren und zu beseitigen (Security by Design). Die infrastrukturelle Verbindung von sehr vielen individuellen Komponenten zu großen komplexen Systemen dient unter anderem der Industrie 4.0 als Basis für intelligente Fabriken und Fertigungsprozesse, die sich in kürzester Zeit dynamisch an neue Aufgaben anpassen können. Der Austausch sensibler Informationen, wie beispielsweise von Firmengeheimnissen, muss auch in solch hochkomplexen Anwendungsgebieten ohne Gefahr der Spionage möglich sein.

Beratung und Service für Gesellschaft, Politik und Unternehmen

Foto: Thomas Jupa

Cybersicherheit ist essentiell für eine funktionierende Wirtschaft und für nahezu alle Bereiche unserer eng vernetzten Gesellschaft. Dabei entstehen immer neue Abhängigkeiten des Menschen von der einwandfreien Funktionsfähigkeit von Systemen. Cyberattacken zeigen, wie verwundbar heutige Infrastrukturen sind. Dadurch macht sich immer mehr Unsicherheit und Sorge um den Schutz der eigenen Privatsphäre breit.

Die Forschungsergebnisse von CRISP verbessern den Schutz der Privatsphäre der Bürgerinnen und Bürgern und schaffen benutzbare Cybersicherheit. Die Sicherheit großer Systeme ist auch für Industrie und Wirtschaft relevant – CRISP forscht deswegen für mehr Sicherheit bei Entwicklungs- und Produktionsprozessen. Durch die wirtschafts- und technologiepolitische Dimension der Forschungsergebnisse von CRISP sind diese auch für Politikerinnen und Politiker von großer Bedeutung.

Foto: Oliver Dietze

Prof. Dr. Michael Waidner
Fraunhofer SIT

Foto: Hochschule Darmstadt

Prof. Dr. Harald Baier
Hochschule Darmstadt

Foto: TU Darmstadt

Prof. Dr. Johannes Buchmann
TU Darmstadt

Foto: Fraunhofer IGD

Prof. Dr. Dieter W. Fellner
Fraunhofer IGD

Zusammenspiel der Partner

Durch die unterschiedlichen Forschungsschwerpunkte der vier Partner entstehen in CRISP eindrucksvolle Kooperationen und kraftvolle Synergien. So liegen die Kernkompetenzen des Profilbereichs Cybersicherheit (CYSEC) der Technischen Universität Darmstadt in der Forschung und Lehre: In ihren mehr als 30 Forschungsgruppen betreibt die TU Darmstadt sowohl Grundlagen- als auch anwendungsorientierte Forschung. Weitere Schwerpunkte der TU Darmstadt sind die Lehre im Masterstudiengang IT-Sicherheit, die Förderung des wissenschaftlichen Nachwuchses und die Unterstützung von Ausgründungen und Startups.

An der TU Darmstadt sind außerdem mehrere DFG-geförderte Spitzenforschungsprojekte angesiedelt: der deutschlandweit erste Sonderforschungsbereich zum Thema Kryptographie und ein Graduiertenkolleg, das sich mit dem hochaktuellen Thema der Privatheit für mobile Nutzer beschäftigt. Der Chiphersteller Intel fördert an der TU Darmstadt seit vielen Jahren das erste Intel-Forschungszentrum für Cybersicherheit außerhalb der USA. Technologietransfer über nationale und internationale Kooperationen mit außeruniversitären Forschungseinrichtungen und industriellen Partnern runden das Profil von der CYSEC ab.

Entsprechend der Zielsetzung der Fraunhofer-Gesellschaft betreiben die beiden Fraunhofer-Institute exzellente Technologieforschung, oft im Auftrag und in Zusammenarbeit mit Partnern aus Industrie und Verwaltung, und identifizieren und beschreiben wichtige neue Trends und Strategien in der Cybersicherheit. Das Fraunhofer SIT deckt dabei die gesamte Bandbreite der Forschung im Bereich Cybersicherheit und Privatsphärenschutz ab. Ein Großteil der Forschung erfolgt in Kooperation mit führenden akademischen und industriellen Cybersicherheitseinrichtungen in aller Welt. Eine besonders enge Partnerschaft besteht mit der Hebrew University of Jerusalem, mit der zusammen das Fraunhofer SIT ein Fraunhofer-Projektzentrum für Cybersicherheit betreibt. Das Fraunhofer IGD ist die international führende Einrichtung für angewandte Forschung im Visual Computing. Bezüglich Cybersicherheit liegt der Schwerpunkt des Fraunhofer IGD auf den Themenfeldern Biometrie und Visual Analytics.

Durch die Auszeichnung der beiden Fraunhofer-Institute zum Fraunhofer-Leistungszentrum für Sicherheit und Datenschutz in der Digitalen Welt erfährt die Cybersicherheitsforschung am Standort Darmstadt eine weitere Stärkung. Ziel des Ende 2016 eröffneten Leistungszentrums ist es, zum Wohl von Wirtschaft und Gesellschaft beizutragen und sich hierbei auf die Sicherheit von großen realen IT-Systemen zu fokussieren. Das Leistungszentrum betreibt anwendungsorientierte Forschung und vernetzt sich hierzu mit internationalen Universitäten sowie namhaften Unternehmen aus Wirtschaft und Industrie. Kern der Aktivitäten bildet die Entwicklung von Basisbausteinen für mehr Cybersicherheit und den Schutz der Privatsphäre.

An der Hochschule Darmstadt ist Cybersicherheit ein wichtiger Forschungsschwerpunkt. Die Wissenschaftlerinnen und Wissenschaftler beschäftigen sich mit Biometrie, Internetsicherheit, IT-Forensik, benutzbaren Sicherheitslösungen sowie mobilen, sicheren und vertrauenswürdigen Telekommunikationsdiensten zur gegenseitigen Authentifizierung. Mit der Vertiefungsrichtung IT-Sicherheit im Masterstudiengang Informatik, dem kooperativen Studiengang IT-Sicherheit (KITS) und der Beteiligung am Weiterbildungsangebot OpenC3S stärkt die Hochschule Darmstadt nachhaltig das Darmstädter Ausbildungsangebot auf dem Gebiet der Cybersicherheit.

Der Cybersicherheitsstandort Darmstadt zeichnet sich somit besonders durch die enge Kooperation von Lehre und Grundlagenforschung durch die TU Darmstadt und die Hochschule Darmstadt mit der anwendungsnahen Forschung durch die beiden Fraunhofer-Institute SIT und IGD aus.

KASTEL Karlsruhe

Das Kompetenzzentrum für angewandte Sicherheits-Technologie KASTEL

Das „Kompetenzzentrum für angewandte Sicherheits-Technologie“ (KASTEL) untersucht, wie sichere Anwendungen in einem durchgängigen Prozess entwickelt werden können. Unter dem Motto „Nachvollziehbare Sicherheit in der vernetzten Welt“ stellt sich KASTEL besonders denjenigen Herausforderungen der IT-Sicherheit, die durch die fortschreitende Vernetzung einzelner, bisher isoliert betriebener Systeme entstehen. Diese Herausforderungen treten speziell im Bereich der Energiewirtschaft und der Industrie, aber auch der vernetzten, „intelligenten“ Umgebungen hervor.

Als Leuchttürme dienen die Forschungsfelder „Sicherheit und Privatheit für Stromnetze der Zukunft“ und „Beweisbare Sicherheit für komplexe IT-Systeme“. Stromnetze als Stellvertreter für kritische Infrastrukturen veranschaulichen besonders deutlich den Einfluss, den IT-Systeme auf unseren Alltag haben. Beweisbare Sicherheit ermöglicht es, ganze Klassen von Angreifern prinzipiell auszuschließen, darunter auch noch unbekannte.

Weitere Forschungsfelder sind „Sicherheit und Datenschutz für zukünftige Produktionssysteme“ und „Sicherheit und Datenschutz für die zukünftige Lebens- und Arbeitswelt“ und vernetzte Mobilität.

In KASTEL haben sich die großen Akteure der akademischen IT-Sicherheitsforschung in Karlsruhe zusammengeschlossen: Das Karlsruher Institut für Technologie (KIT), das Fraunhofer IOSB und das FZI Forschungszentrum Informatik. In den BMBF-geförderten KASTEL-Projekten kooperieren zwölf Forschungsgruppen aus den Fachbereichen Informatik, Wirtschafts- und Rechtswissenschaften und entwickeln einen ganzheitlichen Ansatz, der die Kompetenzen und Methoden verschiedener Disziplinen integriert.

KASTEL
Institut für Theoretische Informatik
Carmen Manietta
Am Fasanengarten 5
Geb. 50.34
D-76131 Karlsruhe
Tel.: + 49 721 608-44213
Fax: + 49 721 608-55022
E-Mail: crypto-info@iti.kit.edu
https://www.kastel.kit.edu

Foto: KIT

Fast Facts

- Graduiertenkolleg Energiezustandsdaten
- ERC Consolidator Grant „PREP-CRYPTO: Preparing Cryptography for Modern Applications“
- EnergyLab 2.0: großskalige Forschungsinfrastruktur für Energiesysteme
- IT-Sicherheitslabor für die Produktion: Infrastruktur für sichere Industrie 4.0
- Deutsch-französischer Doppelmaster in Kryptographie
- Informatik-Master mit Vertiefung in Cyber-Sicherheit
- 120+ Mitarbeiter
- 270+ Veröffentlichungen

Leuchttürme

Sicherheit und Privatheit für Stromnetze der Zukunft

Unsere Energiesysteme werden in Zukunft grundlegend umgebaut. Solar- und Windenergie wird dezentral und schlecht planbar erzeugt und nur der intensive Einsatz von IT kann die Erzeugung und den Bedarf in Einklang bringen. Dieser verbreitete Einsatz von IT-Systemen bringt gleichzeitig neue Bedrohungen für Wirtschaft und Gesellschaft: Die zur Netzsteuerung erfassten Stromverbrauchsdaten erlauben Rückschlüsse auf private Lebensgewohnheiten und Produktionsvorgänge in der Industrie. Gleichzeitig erhöhen zusätzliche IT-Systeme die Angriffsfläche; eine Manipulation kann zu Störungen, Schäden und langfristigen, großflächigen Stromausfällen führen. Dies macht IT-Sicherheit zu einer Voraussetzung für die Energiewende.
Das Stromnetz muss als Ganzes betrachtet werden, um die Konzepte und Methoden der Informatik und der Elektrotechnik geeignet integrieren zu können. Insbesondere der Datenschutz und die rechtlichen Rahmenbedingungen der Regulierung erfordern auch eine enge Einbindung der Rechtswissenschaften. KASTEL entwickelt interdisziplinär Lösungen, die Sicherheit und Privatheit in den Stromnetzen der Zukunft gewährleisten.

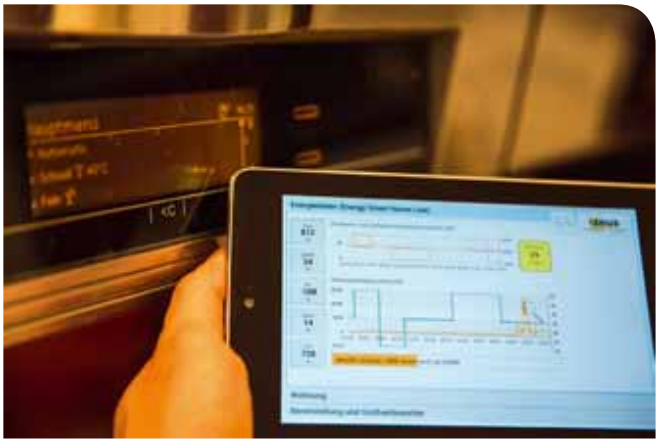


Foto: KIT

Eine besondere Herausforderung ist es, die scheinbar widersprüchlichen Anforderungen an die Funktion, deren Echtzeitfähigkeit, den Schutz der Privatsphäre sowie die Robustheit gegen Angriffe und Störungen miteinander zu vereinbaren. Verteilte Energiesysteme sollen nicht nur über eine sichere IT-Infrastruktur verfügen, sondern auch als Ganzes widerstandsfähig sein, da Angriffe nicht völlig vermieden werden können.
KASTEL erforscht die Sicherheit und Robustheit realer Systeme im Energy Lab 2.0 der Helmholtz-Gemeinschaft und im IT-Sicherheitslabor für die Produktion des Fraunhofer IOSB.

Beweisbare Sicherheit für komplexe IT-Systeme

Sicherheit in modernen, komplexen Systemen kann nur verlässlich sicher gestellt werden, wenn die Anforderungen, die an ein System gestellt werden, vom Design bis hin zur Qualitätssicherung der eigentlichen Implementierung des Systems durchgängig sind. Praktisch beobachtbare Angriffe auf Systeme sind in der Regel auf fehlende Sicherheitskonzeptionen zurückzuführen oder aber auf Fehler, die erst in der Implementierung entstanden sind, so dass das eigentlich angedachte Sicherheitsdesign nicht konsequent umgesetzt wurde.
Deshalb forschen wir in KASTEL an einer Systemtheorie für die kontinuierliche Anpassung an strategische, sich weiterentwickelnde Angreifer, sowie an Werkzeugen und Methoden, die Sicherheit vom Design bis zur letzten Code-Zeile gesamtheitlich betrachten, durchgängig umsetzten und überprüfbar machen. Experten aus den unterschiedlichsten Disziplinen der Informatik arbeiten deshalb eng mit Experten aus den Rechtswissenschaften zusammen, um bekannte Methoden zur Dokumentation und Analyse von Systemen und Programmen weiterzuentwickeln und für den Einsatz im sicherheitskritischen Umfeld nutzbar zu machen.

Die IT-Sicherheitsregion Karlsruhe

Keine andere deutsche Stadt hat eine Informatik-Tradition wie Karlsruhe. Die 1972 gegründete Informatikfakultät an der damaligen Universität Karlsruhe (TH), dem heutigen Karlsruher Institut für Technologie (KIT), ist nicht nur die älteste in Deutschland, sondern belegt seit ihrer Gründung auch Spitzenplätze in allen Rankings. Die gesamte Karlsruher Informatik ist allerdings noch umfassender: Neben dem Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) an der Fakultät für Wirtschaftswissenschaften des KIT gibt es das FZI Forschungszentrum Informatik, das mit dem FZI House of Living Labs eine einzigartige Forschungsumgebung für die gesamte Informatik-Anwendungsforschung bietet, und das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) mit seinem deutschlandweit einzigartigen Sicherheitslabor für die industrielle Produktion. Alle drei Institutionen komplementieren die Informatikfakultät in Richtung angewandter Informatik und Technologietransfer.

Der Standort Karlsruhe, IKT-Schwerpunkt Nummer zwei in Deutschland (Nummer vier in Europa), ist ein Zentrum der deutschen IT-Wirtschaft. Ausdruck davon ist nicht zuletzt das Cyberforum, mit über 1000 Unternehmensmitgliedern Europas größtes regional aktives Hightech-Unternehmer-Netzwerk, das mit der Karlsruher IT-Sicherheitsinitiative KA-IT-Si über eine eigene Special Interest Group für IT-Sicherheit verfügt. In der TechnologieRegion Karlsruhe arbeiten über 30.000 Menschen in der IKT-Branche.

Die TechnologieRegion selbst ist eingebettet in die „Software-Cluster-Region“ (Rhein-Main-Neckar). Die etwa 11.000 Software-Unternehmen dieser Region mit zusammen über 120.000 Mitarbeitern erwirtschaften gemeinsam einen Jahresumsatz von 25 Milliarden Euro und stellen 40% der weltweiten Entwicklung von betrieblicher Individualsoftware dar.

Foto: KIT

Fast Facts

- 30.000+ Beschäftigte in der IT-Branche
- 4.200+ IT-Unternehmen
- 10 außeruniversitäre Forschungseinrichtungen
- 5+ Mrd. Euro Jahresumsatz in der IT-Branche
- Testfeld Autonomes Fahren

Die enge Zusammenarbeit von KASTEL mit dem Kompetenzzentrum IT-Sicherheit des FZI, dem Digitalen Innovationszentrum und der Karlsruher IT-Sicherheitsinitiative KA-IT-Si sowie die zahlreichen Industriekooperationen von KASTEL belegen, welche Bedeutung die Kooperation zwischen Forschung und Industrie für KASTEL und die in Karlsruhe angesiedelten Firmen hat.

Foto: Fraunhofer IOSB

Sicherheit und Datenschutz für zukünftige Produktionssysteme

Moderne industrielle Produktionsanlagen, die dem Konzept „Industrie 4.0“ folgen, sind im Gegensatz zu den früheren alleinstehenden Anlagen vernetzt, weil sie für ihr Funktionieren mit anderen Systemen Daten austauschen müssen. Damit werden neue Arten von Angriffen möglich. In Industrie-4.0-Szenarien werden zudem vermehrt intelligente autonome Komponenten zum Einsatz kommen, die spontan mit bereits produktiven Komponenten interagieren. Sicherheit in diesen Anlagen muss umfassend von der Planungsebene bis auf die technischen Ebenen betrachtet werden, auf denen Anlagen über Sensoren und Aktoren durch speicherprogrammierbare Steuerungen und ähnliche echtzeitkritische Komponenten betrieben werden.

In KASTEL werden innovative und zukunftsfähige Forschungsfragen für industrielle Produktionsanlagen untersucht, die auf allen Systemebenen sicher sind. Neben rechtlichen Aspekten des Datenschutzes sind dies zukünftige, flexible Sicherheitskonzepte für Industrie 4.0, die sichere Cloud-Nutzung für Industrie 4.0, eine selbstlernende Anomalieerkennung in der industriellen Produktion, Echtzeitanforderungen unter Angriffen und nachweisbare Sicherheit in Anwesenheit von Angreifern.

Sicherheit und Datenschutz für die vernetzte Mobilität

Die Digitalisierung hat schon lange Einzug in den Verkehr gehalten und wird ihn in Zukunft weit stärker beeinflussen. Fahrzeuge enthalten eine Vielzahl miteinander vernetzter Steuergeräte und Unterhaltungselektronik. Durch aktuelle Informationen anderer Verkehrsteilnehmer verbesserte Routenplanung ist schon jetzt verfügbar. Elektromobilität und automatisiertes Fahren werden in absehbarer Zukunft Realität. Alle diese Entwicklungen bringen auch Bedrohungen für die Sicherheit und die Privatsphäre der Nutzer mit sich.

KASTEL-Forscher entwickeln datenschutzfreundliche Techniken für Routenplanung. Im Bereich Elektromobilität untersuchen sie die Sicherheit von Standards und Protokollen und beschäftigen sich mit sicheren und privatsphärenfreundlichen Vehicle-to-Grid-Lösungen. Weiterhin ist KASTEL an der Profilregion Mobilitätssysteme Karlsruhe beteiligt und befasst sich dort mit der Sicherheit vernetzter Mobilität.

Forschungsthemen

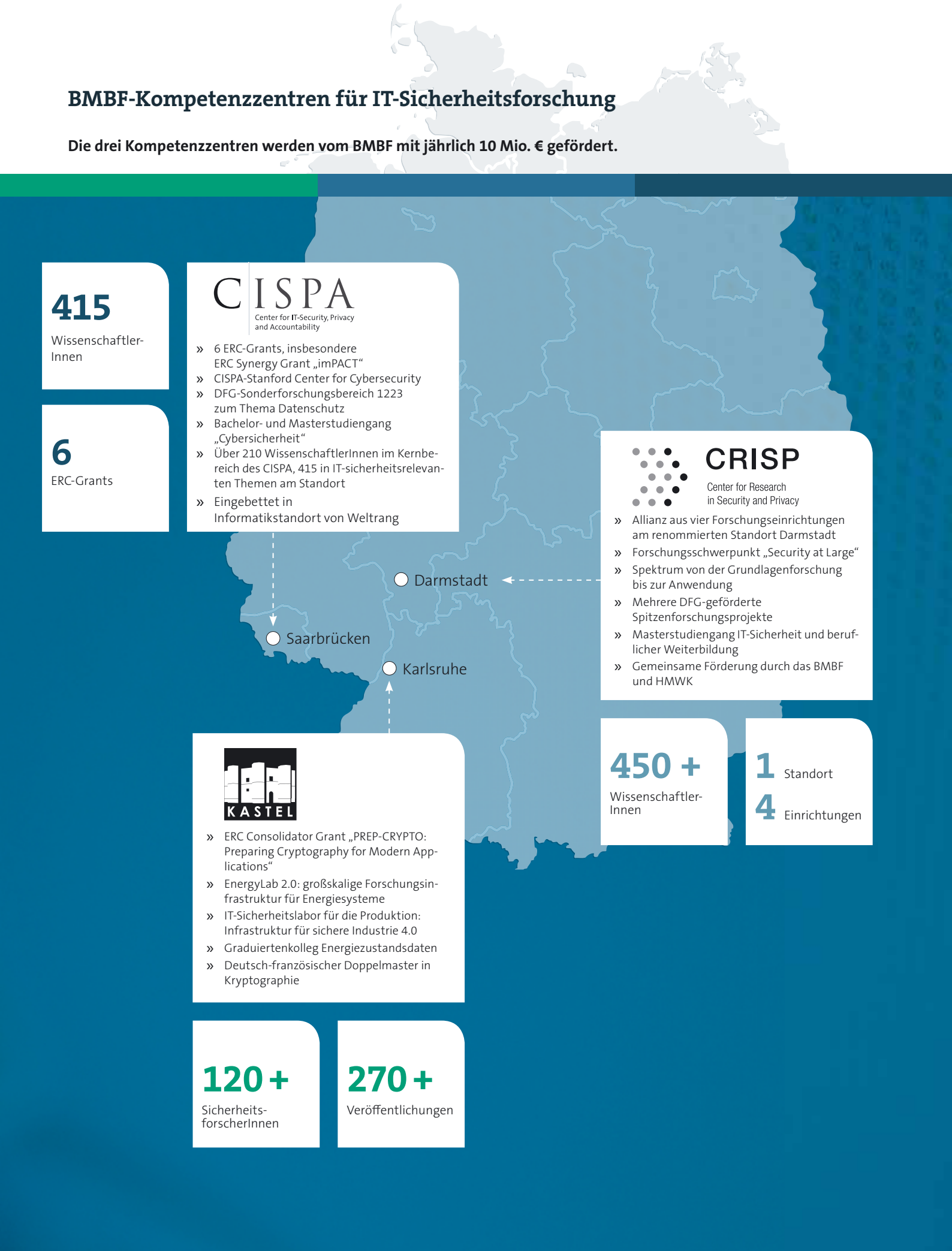
Sicherheit und Datenschutz für die zukünftige Lebens- und Arbeitswelt

Die tiefgreifende Integration von IT in die Lebens- und Arbeitswelt ermöglicht eine Vielzahl innovativer Anwendungen und Dienste. In Smart Environments bilden vernetzte Sensoren und Aktoren die Grundlage für eine Automatisierung alltäglicher Abläufe, mehr Komfort und eine effiziente Nutzung von Ressourcen. Damit einher geht eine allgegenwärtige Erfassung und Verarbeitung von Daten, die insbesondere auch den Kernbereich der persönlichen Lebensgestaltung betrifft. So kann aus den erfassten Daten auf Tätigkeiten, Interessen und Vorlieben von Personen oder Organisationen geschlossen werden. Eine der großen Herausforderungen von Smart Environments liegt somit im Schutz der Privatsphäre bzw. von Geschäftsgeheimnissen.

Für Sicherheit und Datenschutz in der zukünftigen Lebens- und Arbeitswelt erforscht KASTEL verschiedene Konzepte und Verfahren. Dazu zählen eine Architektur für eine Datenschutz-respektierende Lagedarstellung bei Großveranstaltungen, ein Konzept für eine Datenschutz-konforme Erhebung und Visualisierung von Sensordaten, dezentrale elektronische Währungen und Lösungsansätze für die Delegation von Sicherheitsaufgaben bei ressourcenschwachen Geräten, eine Weiterentwicklung von Datenschutzkonzepten für intelligente Umgebungen, Identitätsmanagement und Nutzungskontrolle über verschiedene Kontexte ohne gemeinsamen Vertrauensanker und Software-Integritätsprüfungen ohne vertrauenswürdige Instanz.

BMBF-Kompetenzzentren für IT-Sicherheitsforschung

Die drei Kompetenzzentren werden vom BMBF mit jährlich 10 Mio. € gefördert.



415
Wissenschaftler-Innen

6
ERC-Grants

CISPA
Center for IT-Security, Privacy and Accountability

- 6 ERC-Grants, insbesondere ERC Synergy Grant „imPACT“
- CISPA-Stanford Center for Cybersecurity
- DFG-Sonderforschungsbereich 1223 zum Thema Datenschutz
- Bachelor- und Masterstudiengang „Cybersicherheit“
- Über 210 WissenschaftlerInnen im Kernbereich des CISPA, 415 in IT-sicherheitsrelevanten Themen am Standort
- Eingebettet in Informatikstandort von Weltrang

CRISP
Center for Research in Security and Privacy

- Allianz aus vier Forschungseinrichtungen am renommierten Standort Darmstadt
- Forschungsschwerpunkt „Security at Large“
- Spektrum von der Grundlagenforschung bis zur Anwendung
- Mehrere DFG-geförderte Spitzenforschungsprojekte
- Masterstudiengang IT-Sicherheit und beruflicher Weiterbildung
- Gemeinsame Förderung durch das BMBF und HMWK

450 +
Wissenschaftler-Innen

1 Standort
4 Einrichtungen

KASTEL

- ERC Consolidator Grant „PREP-CRYPTO: Preparing Cryptography for Modern Applications“
- EnergyLab 2.0: großskalige Forschungsinfrastruktur für Energiesysteme
- IT-Sicherheitslabor für die Produktion: Infrastruktur für sichere Industrie 4.0
- Graduiertenkolleg Energiezustandsdaten
- Deutsch-französischer Doppelmaster in Kryptographie

120 +
SicherheitsforscherInnen

270 +
Veröffentlichungen