LIEBE LESER:INNEN,

Die großen Probleme der Menschheit kennen keine Grenzen. Egal ob Klimakrise, zwischenstaatliche Konflikte oder die fragile Sicherheit des Internets – das alles sind komplexe, interdependente Herausforderungen, die uns alle betreffen und die wir nur gemeinsam bewältigen können.

Als weltweit führendes Zentrum der Cybersicherheit haben wir am *CISPA* verstanden, dass es für ein sicheres Morgen auch in der Forschung keine Grenzen geben kann. Informationssicherheit, Datenschutz und vertrauenswürdige künstliche Intelligenz sind die Eckpfeiler unserer (digitalen) Zukunft und noch immer große Herausforderungen. Unsere exzellenten Wissenschaftler:innen arbeiten daher in vielen Projekten mit internationalen Expert:innen aus Forschung, Industrie und Wirtschaft zusammen, um sich ihrer Aufgabe zu stellen und die Welt ein Stück sicherer zu machen.

Und wir gehen voran: Im von uns koordinierten Projekt *ELSA – European Lighthouse on Secure and Safe AI* bauen wir gerade ein großes Exzellenz-Netzwerk von KI-Expert:innen in ganz Europa auf. Zusammen mit *Inria* in Paris und *Loria* in Nancy haben wir zudem im Jahr 2020 das *Deutsch-Französische Zentrum für Cybersicherheit* gegründet und bündeln unsere Kräfte, um die Innovationsaktivitäten Deutschlands und Frankreichs zu stärken. Das sind nur zwei Beispiele unserer gelungenen grenzüberschreitenden Zusammenarbeit, mit dem Ziel, eine sichere digitale Ära zu gestalten. Mit wem das *CISPA* und seine Forschenden noch zusammenarbeiten und welche brennenden Probleme dabei gelöst werden, lesen Sie in dieser neuen Ausgabe des Zines.

Prof. Dr. Dr. h. c. Michael Backes © Tobias Ebelshäuser

Viel Spaß beim Lesen!

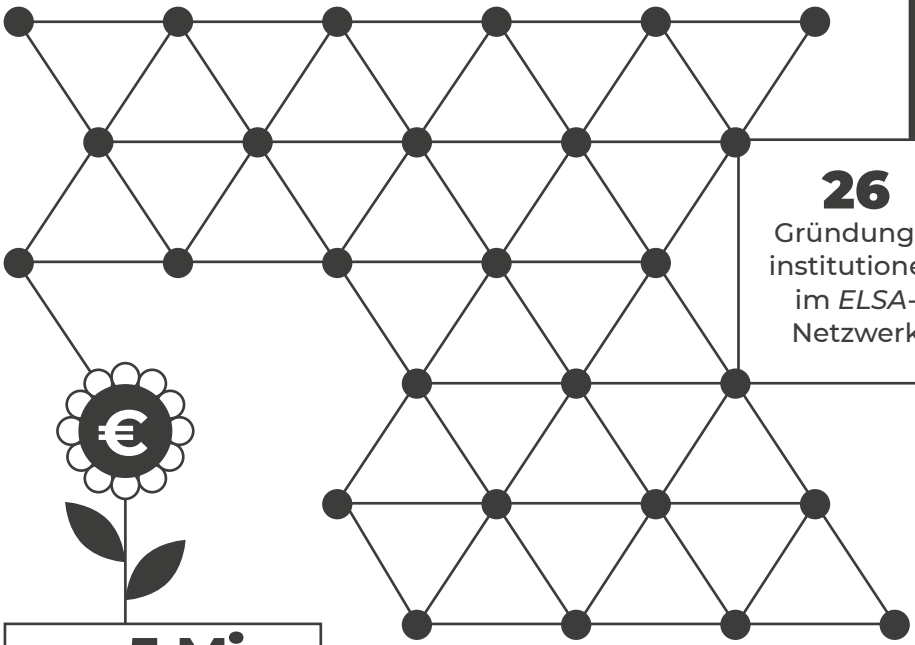
Prof. Dr. Dr. h. c. Michael Backes

FACTS ABOUT CISPA

Information vom: 2024/02

Gründungsjahr des *Deutsch-Französischen Zentrums für Cybersicherheit:*

2020



26
Gründungs-institutionen im *ELSA*-Netzwerk

ca. 5 Mio.
Förderung der EU für das Projekt *TESTABLE*

8 bis 12
Wochen ist die Dauer des *CISPA Summer Voluntary Internship Program*

INTERNATIONALE ZUSAMMENARBEIT AM CISPA

Weltweit nimmt die Vernetzung von Menschen und Systemen zu. Die Erforschung der Sicherheit des digitalen Raumes und der Vertrauenswürdigkeit künstlicher Intelligenz darf daher nicht an nationalen Grenzen halt machen. „Am *CISPA* ist der Austausch mit internationalen Expert:innen auf verschiedenen Gebieten gelebte Praxis“, erklärt Miriam Menzel. Sie arbeite lange im *Project Office* des *CISPA* und koordinierte unter anderem die Zusammenarbeit im *Deutsch-Französischen Zentrum für Cybersicherheit (FGCC)*, das 2020 gegründet wurde. Zu den zentralen Forschungsthemen des Zentrums gehören europäische Internet- und Kryptographie-Standards, in Europa entwickelte Betriebssysteme zur Sicherung kritischer Infrastrukturen und der Privatsphäreschutz. *CISPA-Faculty Prof. Dr. Antoine Joux* ist auf deutscher Seite wissenschaftlich federführend für das *FGCC* verantwortlich und sicher: „Diese Zusammenarbeit ermöglicht nicht nur bahnbrechende Forschung, sondern lässt auch die deutsch-französische Freundschaft wachsen.“

Was im Kleinen geht, geht auch im Großen: Im wachsenden Exzellenznetzwerk *ELSA – European Lighthouse on Secure and Safe AI* sind Forschende und Industriepartner:innen aus vielen Ländern Europas verbunden. Koordiniert wird *ELSA* von *CISPA-Faculty Prof. Dr. Mario Fritz*. Er will mit dem Netzwerk viel bewegen: „Künstliche Intelligenz hat das Potential, unser aller Leben enorm zu verbessern – sei es durch eine bessere Gesundheitsversorgung oder völlig neue Möglichkeiten der Mobilität. Aber aus einem Segen kann schnell ein Fluch werden, wenn die Technologie nicht auf einem sicheren Fundament basiert. Ich sehe enormes Potential, durch *ELSA* die Top-Forschenden Europas zusammenzubringen, um uns gemeinsam den großen Herausforderungen von KI und maschinellem Lernen zu stellen.“

Neben der Bündelung von Kompetenzen ist für *CISPA-Forscherin Lea Gröber* noch ein anderer Aspekt internationaler Zusammenarbeit in der Forschung wichtig: „Andere Regionen und Länder der Welt haben einen ganz anderen soziokultu-

Dr. Katharina Krombholz © Lea Gröber

Dr. Katharina Krombholz auf Forschungsreise in Lahore.

rellen Hintergrund als wir hier in Deutschland und Europa. Und so sind ihre Cybersicherheitsrisiken und Bedürfnisse oft auch völlig andere.“ Gröber forscht in der Gruppe von *CISPA-Faculty Dr. Katharina Krombholz* an sogenannter *Usable Security*. „Unsere Forschung ist sehr nutzer:innenzentriert, deshalb ist es für uns wichtig, die Population in ihrer gesamten Bandbreite zu betrachten. Alle Menschen haben das Recht auf ein sicheres Internet.“ Zusammen mit Krombholz ist Gröber schon mehrfach nach Pakistan gereist. „Ich bin über einen Kollegen von der *Universität des Saarlandes*, *Dr. Nida Bajwa*, ins Projekt *Recypher* gekommen“, erklärt Krombholz. Forschende der *Uni des Saarlandes* und des *CISPA* arbeiten darin gemeinsam mit Kolleg:innen von vier pakistanischen Partneruniversitäten daran, an ausgewählten Unis in Pakistan Cybersecurity-Awareness-Zentren zu schaffen, pakistanische Studierende mit Unternehmen im IT-Sicherheitsbereich zu vernetzen und ihnen so die Möglichkeit zu geben, in dieser Branche zu arbeiten. Krombholz hat laut eigener Aussage in Pakistan schon mit herausragenden Nachwuchsforscher:innen gearbeitet. „Ein Großteil der Bewerber:innen, die von Unis in Pakistan kommen, werden an den Elfenbein-Unis in Amerika angenommen, weil sie so gut sind. Wir sprechen in Deutschland ständig über den Fachkräftemangel. Wir sollten versuchen, gute Leute von dort zu uns zu holen“, sagt Krombholz.

Einen guten Einblick in die Forschung am CISPA erhalten Forschende aus Süd-Asien auch durch das *CISPA Summer Voluntary Internship Program*. Für acht bis zwölf Wochen können Studierende, die Interesse an Forschungsfragen aus den Bereichen Cybersecurity, maschinelles Lernen, Datenschutz, Kryptographie, formale Methoden und verwandten Themen haben, ans *CISPA* kommen und von erfahrenen Forschenden gecoacht werden. Denn auch in der Forschung ist Vernetzung immens wichtig.

„MIT VEREINTEN KRÄFTEN ZU MEHR TESTBARKEIT“

Pluribus One, SAP, Norton LifeLock *(vormals* Symantec*), die* TU Braunschweig, Eurecom, Shiftleft, IMQ Minded Security, UC3M *und nicht zuletzt das* CISPA*: Vielmehr namhafte Institutionen aus der Industrie und der akademischen Welt lassen sich gar nicht an einen Tisch bringen. Im mit fast fünf Millionen Euro von der EU geförderten Projekt* TESTABLE *arbeiten sie alle gemeinsam an einem großen Ziel. Welches das ist und wozu es diese geballte Expertise braucht, erklärt uns Projektleiter und* CISPA-Faculty Dr. Giancarlo Pellegrino.

Dr. Giancarlo Pellegrino © Tobias Ebelshäuser

Hallo Giancarlo. Vielleicht gleich zum Einstieg die wichtigste Frage: Was ist die Vision deines Projekts *TESTABLE*?

Wir machen mit *TESTABLE* im Grunde das, was wir schon immer tun: Wir suchen Schwachstellen in Computer-Programmen. Diese sollen nicht mit Problemen oder Sicherheitslücken an Nutzer:innen weitergegeben werden. Es gibt schon viele Tools und Techniken, mit denen wir den Code und die Programmfunktionen untersuchen und so Fehler und Schwachstellen finden können. Diese Tools stoßen aber ständig an Grenzen und Hindernisse. Es sieht so aus, als ob wir uns mit den existierenden Lösungen langsam in einer Sackgasse befinden. Deshalb verfolgen wir mit *TESTABLE* einen ganz neuen Ansatz. Wir haben uns gefragt, woran es liegt, dass die Tools noch so viele Schwachstellen übersehen. Eine Ursache konnten wir klar identifizieren: die Art wie Entwickler:innen Code schreiben. Wir bauen daher im Projekt eine Datenbank auf, in der solche Problemfälle gesammelt sind. In einem nächsten Schritt könnte man sich dann anschauen, wie sich der Code besser schreiben lässt.

In diesem Projekt kollaborieren viele europäische Institutionen aus Forschung und Industrie. Spielt die Internationalität der Teilnehmenden eine Rolle für den Erfolg?

Europäische Projekte geben einem die konkrete Möglichkeit, zusammenzuarbeiten und sind gut für die Vernetzung und den Erfahrungsaustausch. Innerhalb des großen Ganzen gibt es viele kleine Projekte, zum Beispiel zwischen *CISPA, SAP* und der *TU Braunschweig*, aus denen dann Paper entstehen. Die Projekttreffen sind das Hauptelement, das es uns ermöglicht, diese Zusammenarbeit aufzubauen. Wir treffen uns, halten Workshops ab, stellen unsere Ergebnisse vor, präsentieren frische Ideen und suchen konstant Möglichkeiten, zusammenarbeiten.

Wie funktioniert die Zusammenarbeit mit Industriepartnern wie *SAP* oder *Norton*?

Wir haben einen gemeinsamen Plan, wie wir Programme sicherer machen können. *CISPA* treibt beispielsweise den Stand der Technik im Bereich der automatisierten Sicherheitstests voran. *UC3M* tut dasselbe, jedoch im Bereich Privacy und Datenschutz. *Eurecom* leitet die Erstellung des Datensatzes für Testbarkeitsmuster. *Pluribus One* kümmert sich um maschinelles Lernen. *SAP, Shiftleft, IMQ Minded Security* und *Norton* sind unsere Industriepartner – sie liefern uns Fallstudien und betreiben auch selbst Forschung, alles mit erstklassigen Forschenden. *Shiftleft* ist dafür verantwortlich, potenzielle industrielle Anwendungsfälle für die von uns entwickelten Technologien zu identifizieren. *Norton* konzentriert sich auf die Datenschutzanforderungen der Benutzer, und *SAP* auf Sicherheitstests. *Shiftleft* stellt Testwerkzeuge her, die wichtig sind, um unsere neu entwickelten Ansätze zu testen. *IMQ Minded Security* übernimmt eine beratende Rolle. Sie sind am ehesten in der Lage, uns mitzuteilen, wie unsere Konzepte in der Industrie umgesetzt werden können. Jeder Partner leistet seinen eigenen Beitrag.

Ich wollte dich eigentlich fragen, was die Herausforderungen bei einer solchen Zusammenarbeit sind. Aber was du mir bisher erzählt hast, klingt sehr angenehm.

Glücklicherweise gibt es nicht viele. Wenn ich eine auswählen müsste... könnte ich dir von der größten erzählen: die Entscheidung über den Ort für das nächste Projektmeeting! Wir haben Partner aus vielen schönen Orten in Europa. Wir entscheiden immer strategisch, basierend darauf, wie das Wetter sein wird.

Das Interview führte Annabelle Theobald. Das gesamte Gespräch gibt es unter: https://cispa.de/testable

DAS FEIERN WIR!

Am 6. November 2023 starteten in Paris Forschende des *CISPA* und des französischen Forschungsinstituts *Inria* mit einem Kick-Off-Workshop zu IT-Sicherheitsthemen in die Arbeitsphase einer bereits im Juli beschlossenen Kooperation der beiden Leuchttürme der Cybersicherheit. Workshopteilnehmerin und *CISPA-Faculty Dr. Aurore Fass* ist überzeugt, dass diese Bündelung von Wissen und Ressourcen Innovation und Technologietransfer weltweit fördern wird.

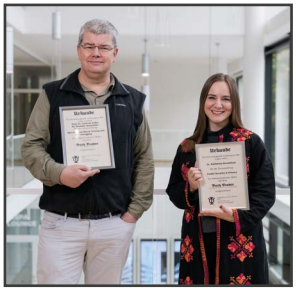
© Foto Inria

Max Wolf
© Tobias Ebelshäuser

Der Technologietransfer am *CISPA* startete 2023 mit einem Rekord an Startup-Förderungen und innovativen Programmen durch, um den Strukturwandel im Saarland voranzutreiben. 2023 unterstützte der *CISPA-Inkubator* mehr als zehn neue Startups, was die Gesamtzahl der betreuten Teams auf über 30 erhöht. Eine kürzlich veröffentlichte *IHK*-Studie unterstreicht die Leistungsfähigkeit des Innovationsökosystems und weist den Ausgründungen aus dem *CISPA* ein hohes Potenzial zu. Ab 2030 werden jährlich erwartbare regionalwirtschaftliche Effekte von 133,4 Millionen Euro allein durch *CISPA-Startups* prognostiziert.

Das Exzellenznetzwerk *ELSA – European Lighthouse on Secure and Safe AI* hat in seinem ersten Jahr wichtige Weichen gestellt, um die Europäische Union zu einem Leuchtturm sicherer und vertrauenswürdiger künstlicher Intelligenz zu machen. Ein wichtiger Meilenstein des Projektes war die Veröffentlichung seiner strategischen Forschungsagenda im November 2023. Ein weiterer Erfolg ist die Entwicklung der *ELSA-Benchmarks-Plattform*. Sie hilft Spitzen-Forschenden in ganz Europa, ihre entwickelten Technologien und Methoden unter realen Bedingungen zu testen und deren Anwendungsreife zu bewerten.

Dr. Mario Fritz
© Annabelle Theobald



Prof. Dr. Andreas Zeller
und Dr. Katharina Krombholz
© Tobias Ebelshäuser

Herzlichen Glückwunsch an *CISPA-Faculty Prof. Dr. Andreas Zeller*, *CISPA-Forscher Dominic Steinhöfel* und *CISPA-Faculty Dr. Katharina Krombholz*! Für ihre herausragende Lehre im Sommersemester 2023 sind die Forschenden mit dem *Busy-Beaver-Award* ausgezeichnet worden. Der Fachschaftsrat der Informatikstudiengänge an der *Universität des Saarlandes* verleiht die Auszeichnung zweimal jährlich an Dozierende, die durch besonderes Engagement auf sich aufmerksam gemacht haben.

Herausgeber:
CISPA – Helmholtz-Zentrum
für Informationssicherheit gGmbH
Stuhlsatzenhaus 5
66123 Saarbrücken, Deutschland

Verantwortliche Redaktion:
Sebastian Klöckner

Redaktion:
Annabelle Theobald

Design:
Lea Mosbach,
Janine Wichmann-Paulus

Stand des Impressums:
Februar 2024

Fotografie:
Tobias Ebelshäuser,
Lea Gröber,
Annabelle Theobald

Kontakt Unternehmenskommunikation:
T: +49 681 87083 2867
M: pr@cispa.de
W: https://cispa.de/

CISPA

DE

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

ZINE 6

Deutsche Edition

TESTABLE

Was ist TESTABLE?

TESTABLE ist ein von der EU gefördertes Projekt, mit dem moderne webbasierte und KI-gestützte Anwendungssoftwaresysteme sicher und datenschutzfreundlicher erstellt und gepflegt werden können.

Was ist das Ziel von TESTABLE?

Das Projekt legt den Grundstein für eine bessere Integration von Sicherheit und Datenschutz bei der Softwareentwicklung.

Partner:

CISPA, EURECOM, TU Braunschweig, Universidad Carlos III de Madrid (UC3M), SAP, ShiftLeft GmbH, IMQ Minded Security, NortonLifeLock (a.k.a. Symantec), Pluribus One

Weitere Informationen:

https://testable.eu/vision/

ELSA – EUROPEAN LIGHTHOUSE ON SECURE AND SAFE AI

Was ist ELSA?

ELSA ist ein von der EU gefördertes und von *CISPA-Forscher Prof. Dr. Mario Fritz* koordiniertes, virtuelles Exzellenzzentrum, das die Forschung auf dem Gebiet der sicheren Methoden für künstliche Intelligenz (KI) vorantreibt.

Was ist das Ziel von ELSA?

Als großes und wachsendes Netzwerk europäischer Spitzenexpert:innen für KI und maschinelles Lernen soll *ELSA* die Entwicklung und den Einsatz modernster KI-Lösungen in der Zukunft fördern und Europa zum weltweiten Leuchtturm der KI machen.

Partner:

ELSA hat 26 Gründungsmitglieder, darunter neben akademischen Spitzenpartnern wie der *University of Oxford*, der *EPFL* in Lausanne und *CISPA* auch große Industriepartner wie *Pluribus One*, *Leonardo* und *NVIDIA*.

Weitere Informationen:

https://www.elsa-ai.eu

DEUTSCH-FRANZÖSISCHES ZENTRUM FÜR CYBERSICHERHEIT

Was ist das FGCC?

Das *FGCC* ist ein Zusammenschluss von zwei der größten und renommiertesten Forschungszentren für Cybersicherheit in Europa. Das *CISPA* und *Loria* in Nancy gehen seit 2020 gemeinsame Wege in der Cybersicherheitsforschung.

Was ist das Ziel des FGCC?

CISPA und *Loria* forschen gemeinsam an drängenden Fragen der Cybersicherheit und widmen sich der Stärkung der Transfer- und Innovationsaktivitäten zwischen Frankreich und Deutschland.

Weitere Informationen:

Loria ist die französische Abkürzung für *Lorraine Research Laboratory in Computer Science and its Applications* und ist eine gemeinsame Forschungseinheit des *CNRS*, der *Universität Lothringen* und des *Inria* (*Institut national de recherche en sciences et technologies du numérique*), mit dem das *CISPA* kürzlich seine Kooperation intensiviert hat.

CISPA SUMMER VOLUNTARY INTERNSHIP PROGRAM (SOUTH ASIA)

Was ist das CISPA Summer Voluntary Internship Program (South Asia)?

Es handelt sich um ein *CISPA*-Sommerpraktikum, das motivierten Studierenden aus für eine Dauer von 8 bis 12 Wochen die Möglichkeit bietet, an wissenschaftlichen Cybersecurity-Projekten zu arbeiten, komplexe Forschungsfragen zu analysieren und dabei von erfahrenen Forschenden betreut und gecoacht zu werden.

Was ist das Ziel des Internship Programms?

Wir wollen den wissenschaftlichen Nachwuchs fördern, indem wir hochmotivierten Studierenden mit einem starken Interesse an Forschungsfragen aus den Bereichen Cybersicherheit, maschinelles Lernen, Datenschutz, Kryptographie, formale Methoden und Elektrotechnik Einblicke in die Forschung am *CISPA* bieten.

Weitere Informationen:

https://jobs.cispa.saarland

CISPA