DEAR READER,

Humanity's greatest challenges know no boundaries. Whether it's the climate crisis, interstate conflicts or fragile internet security – all these are complex, interdependent challenges that affect us all and that we can only overcome together.

As the world's leading center for cybersecurity, we at *CISPA* understand that research cannot stop at national borders if we are to build a secure tomorrow. Information security, data protection and trustworthy artificial intelligence are the cornerstones of our (digital) future and they remain major challenges. In many projects, our excellent scientists are working together with international experts from research, industry and business to tackle the task of making the world a little more secure.

And we are leading the way: In the project *ELSA-European Lighthouse on Secure and Safe AI*, which *CISPA-Faculty Professor Dr. Mario Fritz* is coordinating, we are currently building a large network of excellence that brings together AI experts from across Europe. In 2020, we founded the *French-German Center for Cybersecurity* together with *Inria* in Paris and *Loria* in Nancy, joining our forces to strengthen innovation activities in Germany and France. These are just two examples of our successful cross-border cooperations that aim at shaping a secure digital era. In this sixth issue of the Zine, you will learn more about who else *CISPA* researchers are cooperating with and what burning issues we are solving together.

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

I hope you enjoy reading it.

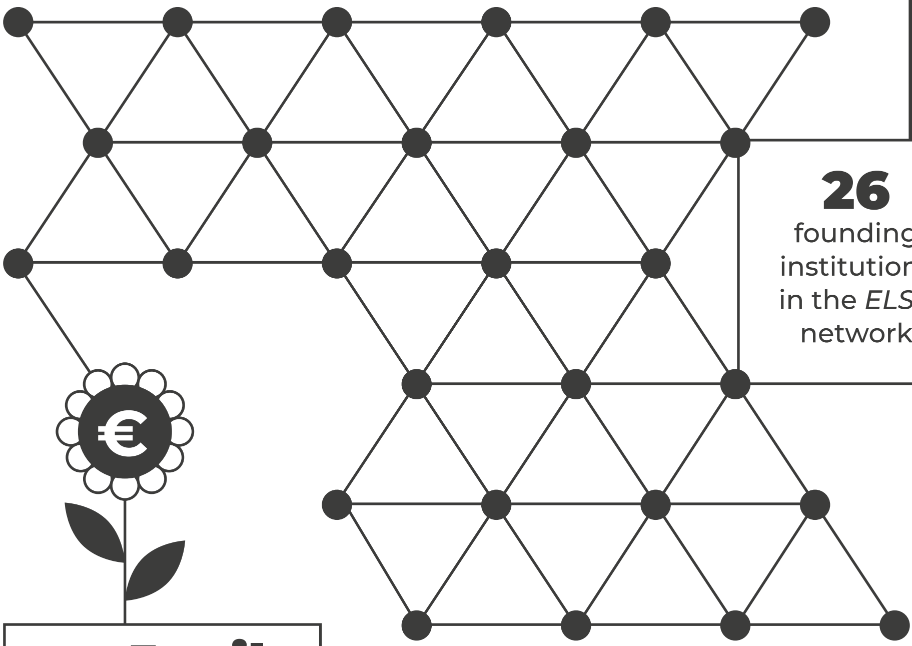
Prof. Dr. Dr. h. c. Michael Backes

FACTS ABOUT CISPA

Information vom: 2024/02

Founding year of the *French-German Center for Cybersecurity:*

2020



26

founding institutions in the *ELSA* network

ca 5 mil.

EU funding for the *TESTABLE* project

8 to 12

weeks is the duration of the *CISPA Summer Voluntary Internship Program*

INTERNATIONAL COOPERATION AT CISPA

People and systems are increasingly interconnected across the globe. For this reason, research into the security of the digital space and the trustworthiness of artificial intelligence cannot stop at national borders. “At *CISPA*, the exchange with international experts in various fields is part of everyday life”, explains Miriam Menzel. She worked at the *CISPA Project Office* and, among other things, coordinated cooperation in the *French-German Center for Cybersecurity (FGCC)*, which was founded in 2020. The center’s key research topics include European internet and cryptography standards, European operating systems for the protection of critical infrastructures as well as privacy protection. The scientific lead for the *FGCC* on the German side is *CISPA-Faculty Professor Dr. Antoine Joux*. He is certain: “This cooperation not only enables groundbreaking research, but it also fosters the French-German friendship.”

If it works on a small scale, it will also work on a large scale: Called *ELSA-European Lighthouse on Secure and Safe AI*, a growing network of excellence brings together researchers and industry partners from many European countries. *ELSA* is coordinated by *CISPA-Faculty Professor Dr. Mario Fritz*. He wants the network to achieve a lot: “Artificial intelligence has the potential to improve all of our lives enormously – whether through better healthcare or completely new mobility options. But a blessing can quickly turn into a curse if the technology is not based on a secure foundation. I see enormous potential in bringing together Europe’s top researchers through *ELSA* in order to tackle the major challenges of AI and machine learning together.”

In addition to pooling expertise, *CISPA researcher Lea Gröber* also values another aspect of international research cooperation: “Other regions and countries around the world have a very different socio-cultural background to us here in Germany and Europe. Their cybersecurity risks and needs are often completely different.” Gröber is researching so-called *Usable Security* in *CISPA-Faculty Dr. Katharina Krombholz’s*

Dr. Katharina Krombholz © Lea Gröber

Dr. Katharina Krombholz on a research trip to Lahore.

research group. Gröber says: “Our research is very user-centered, which is why it is important for us to look at the population as a whole. Everyone has the right to a secure internet.” Together with Krombholz, Gröber has already traveled to Pakistan several times. “I got involved in the *Recypher* project through a colleague from *Saarland University*, *Dr. Nida Bajwa*”, explains Krombholz. In *Recypher*, researchers from *Saarland University* and *CISPA* are working together with colleagues from four Pakistani partner universities to create cybersecurity awareness centers at selected universities in Pakistan, to connect Pakistani students with companies in the IT security sector and thus to give them the opportunity to work in this industry. According to Krombholz, she has already worked with outstanding young researchers in Pakistan. “The majority of applicants who come from universities in Pakistan are accepted at elite universities in America because they are so good. In Germany, we are keep talking about the shortage of skilled professionals. We should try to attract good people from there”, says Krombholz.

Researchers from South Asia can gain insight into research at *CISPA* through the *CISPA Summer Voluntary Internship Program*. For eight to twelve weeks, students who are interested in research questions relating to cybersecurity, machine learning, data protection, cryptography, formal methods and related topics can come to *CISPA* and be coached by experienced researchers. Networking is immensely important in research, too.

“JOINING FORCES FOR MORE TESTABILITY”

Pluribus One, SAP, NortonLifeLock (formerly Symantec), TU Braunschweig, Eurecom, Shiftleft, IMQ Minded Security, UC3M *and also* CISPA: *It is hardly possible to bring together a greater number of reputable institutions from industry and academe. In* TESTABLE, *a project that the EU is funding with almost five million euros, they are working together to achieve a common goal. What this goal is and why it requires the expertise of multiple actors, explains project leader and* CISPA-Faculty Dr. Giancarlo Pellegrino.

Dr. Giancarlo Pellegrino © Tobias Ebelshäuser

Hello Giancarlo. The most important question up front: What is the vision of your project *TESTABLE*?

With *TESTABLE*, we basically keep doing what we have always been doing: We look for vulnerabilities in computer programs. There are already many tools and techniques to analyze code and program functions and to detect errors and vulnerabilities. But these tools have limitations and keep coming up against obstacles given the growing complexity of programs. This is why we are pursuing a new approach with *TESTABLE*. We have been asking ourselves why testing tools are still overlooking so many vulnerabilities or output false alarms. We were able to identify one big problem: The fashion in which developers write code. In the project, we are building up a database to collect these problematic code patterns for testing tools.

Many European institutions from both industry and academe are collaborating in this project. Does the international dimension of the project play a role in its success?

European projects give you the opportunity to work together and they are also good for networking and exchange. Within this framework, we have many collaborations going on, for example by *CISPA, SAP* and *TU Braunschweig*, that eventually result in scientific publications. The project meetings are the core element that enables us to build up collaborations. We meet, have workshops, present our results, introduce fresh ideas and constantly look for opportunities to collaborate.

When researchers collaborate with industry partners such as *Norton* or *SAP*, how does this cooperation work?

We have a shared plan of what we want to do to make programs more secure. Every partner contributes in their own way to this overall goal. *CISPA*, for example, drives forward the state-of-the-art when it comes to automated security testing. *UC3M* does the same, but in the field of privacy and data protection. *Eurecom* leads the creation of the testability patterns dataset. *Pluribus One* takes care of machine learning. *SAP, Shiftleft, IMQ Minded Security* and *Norton* are our industry partners – they provide us with case studies and also conduct research themselves, all with top-notch researchers. *Shiftleft* is responsible for identifying potential industrial use cases for the technologies we have developed. *Norton* concentrates on user-end privacy, and *SAP* on security testing. *Shiftleft* produces testing tools which is important to test our newly developed approaches. *IMQ Minded Security* is in a consulting role. They are the most likely to tell us how our concepts can be implemented in the industry. Every partner makes a contribution of their own.

I wanted to ask you about the challenges of such a cooperation, but what you have been telling me so far actually sounds very pleasant.

Fortunately, there are not many. If I have to cherry pick one...
I can tell you about the biggest on: deciding the location for the next project meeting! We have partners from many beautiful places in Europe, like Sophia Antipolis, in the South of France, Madrid in Spain, Cagliari and Milan in Italy, and Berlin in Germany. We always decide strategically based on what the weather will be like. Our last meeting was in Madrid, fantastic city!

Giancarlo, thank you for this interview.

The interview was conducted by Annabelle Theobald. For the full interview, please visit: https://cispa.de/en/testable

MORE GOOD NEWS

In Paris on November 6, 2023, researchers of *CISPA* and the French research institute *Inria* held a kick-off workshop on IT security topics, diving into the work phase of their intensified cooperation, which was agreed on in July. *Aurore Fass*, workshop participant and *CISPA-Faculty*, is convinced that the pooling of knowledge and resources of both institutions will promote innovation and technology transfer across the world.

© Foto Inria

Technology transfer at *CISPA* took off in 2023 with a record number of startup funding and innovative programs to drive structural change in Saarland. In 2023, the *CISPA Incubator* supported more than ten new startups, bringing the total number of teams supported to over 30. A recently published *IHK* study underlines the efficiency of the innovation ecosystem and assigns high potential to *CISPA* ventures. By 2030, *CISPA* ventures alone are anticipated to have regional economic effects amounting to 133.4 million euros per year.

Max Wolf
©Tobias Ebelshäuser

In its first year, the *ELSA – European Lighthouse on Secure and Safe AI* network of excellence has prepared the ground for making the European Union a beacon of secure and trustworthy artificial intelligence. An important milestone was the publication of its strategic research agenda in November 2023. Another success is the development of the *ELSA Benchmarks Platform*. It helps top researchers throughout Europe to test the technologies and methods they have developed under real-life conditions and assess their readiness for application.

Professor Dr. Mario Fritz
©Annabelle Theobald

Congratulations to *CISPA-Faculty Professor Dr. Andreas Zeller*, *CISPA Faculty Dr. Mridula Singh*, *CISPA researcher Dominic Steinhöfel* and *CISPA Faculty Dr. Katharina Krombholz!* In 2023, their outstanding teaching performance was honored with the *Busy Beaver Award*. Twice a year, the Computer Science Students' Council at *Saarland University* awards the *Busy Beaver* to lecturers who have shown a special commitment to teaching.

Professor Dr. Andreas Zeller
and Dr. Katharina Krombholz
©Tobias Ebelshäuser

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

Editor-in-Chief:
Sebastian Klöckner

Editor:
Annabelle Theobald

Design:
Lea Mosbach,
Janine Wichmann-Paulus

Information as of:
February 2024

Photography:
Tobias Ebelshäuser,
Lea Gröber,
Annabelle Theobald

Contact
Corporate Communication:
T: +49 681 87083 2867
M: pr@cispa.de
W: https://cispa.de/

CISPA

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY | CISPA HELMHOLTZ

EN

ZINE 6

English Edition

TESTABLE

What is TESTABLE?
TESTABLE is an EU-funded project with which modern web-based and AI-supported application software systems can be created and maintained securely and in a more data protection-friendly manner.

What is the goal of TESTABLE?
The project lays the foundation for better integration of security and data protection in software development.

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

More information:
https://testable.eu/vision/

FRENCH-GERMAN CENTER FOR CYBERSECURITY

What is the FGCC?
The *FGCC* is a cooperation of two of the largest and most renowned research centers for cybersecurity in Europe. Since 2020, *CISPA* and *Loria* in Nancy have been pursuing joint paths in cybersecurity research.

What is the goal of the FGCC?
CISPA and *Loria* conduct joint research into pressing cybersecurity issues and are dedicated to strengthening the transfer and innovation activities between France and Germany.

More information:
Loria is the acronym for *Lorraine Research Laboratory in Computer Science and its Applications. Loria* is a joint research unit of the *CNRS*, the *University of Lorraine* and *Inria (Institut national de recherche en sciences et technologies du numérique)*, with which *CISPA* recently intensified its cooperation.

ELSA – EUROPEAN LIGHTHOUSE ON SECURE AND SAFE AI

What is ELSA?
ELSA is a virtual center of excellence, funded by the EU and coordinated by *CISPA researcher Professor Dr. Mario Fritz*, which promotes research on secure methods for artificial intelligence (AI).

What is the goal of ELSA?
As a large and growing network of top European experts in AI and machine learning, *ELSA* aims to promote the development and use of state-of-the-art AI solutions and make Europe the global beacon of AI.

Partner:
ELSA has 26 founding members, among which are top academic partners such as the *University of Oxford, the EPFL in Lausanne* and *CISPA* as well as large industry partners such as *Pluribus One, Leonardo* and *NVIDIA*.

More information:
https://www.elsa-ai.eu

CISPA SUMMER VOLUNTARY INTERNSHIP PROGRAM (SOUTH ASIA)

What is the CISPA Summer Voluntary Internship Program (South Asia)?
It is a summer internship at *CISPA* that offers motivated students the opportunity to work on scientific cybersecurity projects, analyze complex research questions and be supervised and coached by experienced researchers for a period of 8 to 12 weeks.

What is the goal of the Internship Program?
We want to promote young scientific talent by offering insights into *CISPA* research to highly motivated students who have a strong interest in research questions relating to cybersecurity, machine learning, data protection, cryptography, formal methods and electrical engineering.

More information:
https://jobs.cispa.saarland

CISPA