PRESS RELEASE

Agentur für Innovation in der
Cybersicherheit GmbH

Michael Lindner
Pressesprecher
Tel.: +49 (0) 151 4415 0645
E-Mail: presse@cyberagentur.de

Willy-Brandt-Straße 87
06110 Halle (Saale)

New encryption solutions increase data security

Feasibility study "Encrypted Computing" handed over to Cyberagentur

Researchers from the CISPA Helmholtz Centre for Information Security and the KASTEL Institute at the Karlsruhe Institute of Technology (KIT) handed over the results of their feasibility study on the topic of "Encrypted Computing" to the Agentur für Innovation in der Cybersicherheit (Cyberagentur) on Monday (21.11.2022).

In December 2021, the Cyberagentur had awarded its first tendered project on the topic of "Encrypted Computing" to the CISPA Helmholtz Centre for Information Security and to the Karlsruhe Institute of Technology (KIT), as subcontractors. A feasibility study was to identify potential "encrypted computing" applications that could be used in the future in the area of internal and external security. The main objective was to determine the security properties and to compare the performance of these procedures depending on their application scenarios.

Encrypted computing and similar technologies are seen as forward-looking approaches to increase data security. "With cryptography, data processing and data protection can be reconciled," says Prof. Dr. Jörn Müller-Quade from the KASTEL Institute at KIT. Until now, the rule in modern cryptography has been that before you can continue working with encrypted data, you have to decrypt it. CISPA faculty Dr. Nico Döttling and Prof. Dr. Jörn Müller-Quade want to change this. Both researchers are experts in the field of encrypted computing, a family of encryption methods with which data can also be processed in encrypted form. Decryption to plain text is only necessary again if the results are to be viewed, but this is not necessary for calculations. Sensitive and security-critical data can thus be analysed, but at the same time kept secret.

In particular, the efficiency of the currently known algorithms for such cryptography is a major problem for research. "Encrypted computing is not a universal solution for secure computing. However, the field still holds enormous potential, especially if even more efficient algorithms are found," says Döttling. Müller-Quade adds: "In particular, it is currently not a universal solution because it may not be efficient enough for some applications. Perhaps there are even principle limits for some applications. We would be happy about a follow-up project. By being open to technology, we can find more efficient solutions for different levels of security."

"Our mission is to promote innovative technologies for applications in internal and external security, but which are still far from being ready for the market," says Robert Seidel, project manager at the Cyberagentur. "Encrypted computing fits very well into this picture. I am pleased that in KASTEL/KIT and CISPA we were able to win two such research-strong partners for our project." The feasibility study is the first step of the Cyberagentur's research activities in the field of encrypted computing. Further research programmes are to follow: "Already next year, we want to advertise with a new call for proposals that cryptologists continue to address our questions," says project manager Dr. Tanja Zeeb.

About CISPA:

The CISPA Helmholtz Centre for Information Security is a major federal research institution within the Helmholtz Association. The scientists research information security in all its facets. They conduct cutting-edge basic research as well as innovative application-oriented research and work on pressing challenges in cyber security, artificial intelligence and data protection. CISPA research results find their way into industrial applications and products that are available worldwide. In this way, CISPA strengthens the competitiveness of Germany and Europe. It also promotes talent and is a cadre for excellently trained specialists and managers for industry. In this way, CISPA also carries its know-how into the future.

About KASTEL:

KASTEL was established as a national competence centre for IT security by the Federal Ministry of Education and Research. Since 1 January 2021, it has been established as a permanent institution at the Karlsruhe Institute of Technology and in the Helmholtz Association.

As one of the leading international research institutions, KASTEL contributes to interdisciplinary research into holistic solutions for the security and data protection of complex networked systems. This spans the arc from basic research to application research, including timely transfer to the economy, society and politics. KASTEL researches the quantification of security and privacy and is guided by the unity of research, teaching and innovation.

About the Cyberagentur:

The Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) was founded in 2020 as a fully in-house company of the Federal Government under the joint leadership of the Federal Ministry of Defence and the Federal Ministry of the Interior and for Home Affairs by the Federal Government with the aim of taking an application-strategy-related and interdepartmental view of internal and external security in the field of cybersecurity. Against this backdrop, the work of the Cyberagentur is primarily aimed at the institutionalised implementation of highly innovative projects that are associated with a high risk with regard to the achievement of objectives, but at the same time can have a very high disruptive potential if they are successful.

The Cyberagentur is headed by Prof. Dr. Christian Hummert as Research Director and Managing Director and Daniel Mayer as Commercial Director.