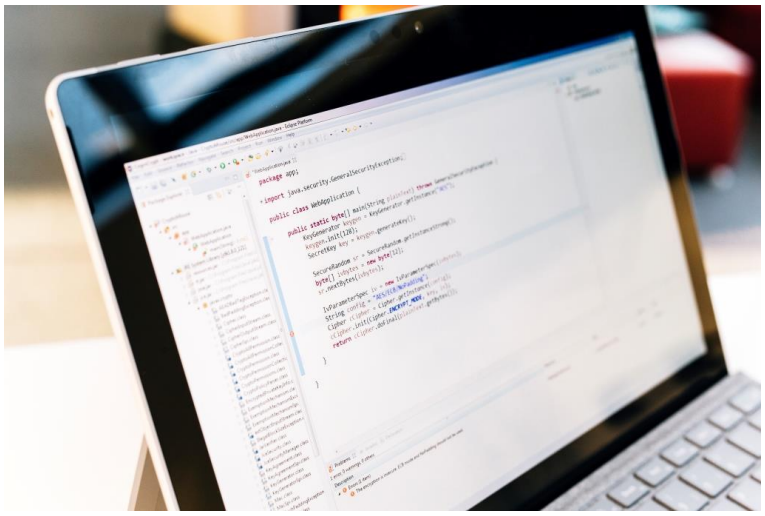
Press release

In a joint CogniCrypt transfer project, Fraunhofer IEM and achelos improve the quality for secure software implementation

There are many potential pitfalls when using cryptographic APIs

Paderborn, 10 July 2019. Veracode published its new State of Software Security Report in January 2019. Producing this report involved analysing over two trillion lines of code over a full year. The results are alarming. More than 85 percent of all applications investigated display at least one weakness, many of which have been occurring for years and often affect cryptography.



The Eclipse CogniCrypt plug-in detects misuse of cryptography directly in the development environment. (Photo: Copyright: Fraunhofer IEM)

This is precisely where the Fraunhofer IEM comes in with CogniCrypt, a tool for static code analysis. The product provides information on the quality of the program code and the cryptographic libraries used. In the "It's OWL" transfer project, Fraunhofer IEM and achelos GmbH spent

four months working together on further developing CogniCrypt. The results were incorporated in the open source product in the form of a knowledge transfer and added support for other cryptographic libraries.

Continuous knowledge transfer in the transfer project

The security experts at achelos incorporated the product in the continuous integration process of their software development operations and tested the tool. achelos was able to contribute its profound cryptographic knowledge within the scope of the project and made a valuable contribution to the development of CogniCrypt. Within the project, CogniCrypt was enhanced by new sets of rules. The new rules allow CogniCrypt to detect security vulnerabilities when using other libraries (Bouncy Castle). The rules defined within the project are fully compliant with Technical Guidelines 02102-1 of the German Federal Office for Information Security (BSI).

CogniCrypt makes software development more secure and high-grade: The tool also supports the experts at achelos during code reviews, as the tool provides proof that the application interfaces (APIs) have been used correctly. "The cryptographic expertise of achelos brought us significant added value in the further development of CogniCrypt," comments Dr. Johannes Späth, Senior Expert at Fraunhofer IEM, summarising the successful cooperation with achelos. "Security and cryptography rank among our core competencies. In the project with Fraunhofer IEM, we were able to incorporate our practical experience in the high-performance tool," adds Kathrin Asmuth, Managing Partner at achelos GmbH.

About CogniCrypt
The CogniCrypt tool was developed within the scope of the CROSSING Collaborative Research Initiative at the Technical University of Darmstadt and in cooperation with the Heinz Nixdorf Institute at the University of Paderborn. It allows companies operating in the field of security and cryptography to identify and then eliminate security-critical misuse of cryptographic libraries quickly and reliably, as well as to generate secure cryptographic integration code for various common usage scenarios fully automatically. With the support of the Fraunhofer IEM, CogniCrypt was further developed to market maturity and can be integrated into the Eclipse development environment.
www.eclipse.org/cognicrypt/

About achelos GmbH:
achelos is a manufacturer-independent software development and consulting firm that is based in the German city of Paderborn. Founded in 2008, the technology expert offers cross-sector solutions for security-critical fields of application with core competencies in embedded development and subscription management. The company develops and operates highly specialised products, solutions and services for the international market. achelos offers comprehensive expertise in development, Testing as a Service (TaaS) and certification.
www.achelos.de | www.IoT.achelos.com

About the Fraunhofer IEM:
From its location in Paderborn, Germany, the Fraunhofer Institute for Mechatronic Systems Design IEM offers expertise for intelligent mechatronic solutions in the context of Industry 4.0. Scientists from the fields of mechanical engineering, software engineering and electrical engineering engage in interdisciplinary collaboration here, researching innovative methods and tools for development of intelligent products, production systems and services.
www.iem.fraunhofer.de/en.html

About the "It's OWL" technology network
In the "It's OWL – intelligent technical systems OstWestfalenLippe" technology network, over 200 companies, research institutes and organisations develop solutions for intelligent products and production methods. With the support of the State of North Rhine-Westphalia, projects with a total value of €100 million are set to be implemented between 2018 and 2022. The key focus topics are artificial intelligence, digital platforms, digital twins and work in the fourth industrial revolution, Industry 4.0. Having won awards in the German government's Top Cluster competition, the "It's OWL" network ranks as one of the largest SME initiatives for Industry 4.0.
www.its-owl.com/home/

Press contact:
achelos GmbH | Daniela Meschede | Vattmannstr. 1 | 33100 Paderborn | Germany
daniela.meschede@achelos.de | T: +49 (0)5251 1421 2345 | M: +49 (0)172 421 1193

Fraunhofer Institute for Mechatronic Systems Design IEM
Zukunftsmeile 1 | 33102 Paderborn | Germany | T: +49 (0)5251 546 5101 |
F: +49 (0)5251 546 5102
Dr. Johannes Späth | johannes.spaeth@iem.fraunhofer.de | T: +49 (0)5251 5465-355
Prof. Dr. Eric Bodden | eric.bodden@iem.fraunhofer.de | T: +49 (0)5251 5465-150