Fraunhofer IEM und achelos haben im CogniCrypt-Transferprojekt Qualität für sichere Softwareimplementierung erhöht. Beim Verwenden von Kryptografie-APIs lauern viele Fallstricke

Im Januar 2019 hat Veracode den neuen State of Software Security Report veröffentlicht. Mehr als zwei Billionen Codezeilen wurden dafür über ein Jahr lang analysiert, die Ergebnisse sind alarmierend. Über 85 Prozent aller untersuchten Anwendungen haben mindestens eine Schwachstelle, viele treten bereits seit Jahren auf und betreffen häufig die Kryptografie. Hier setzt das Fraunhofer IEM mit CogniCrypt, einem Werkzeug zur statischen Code-Analyse, an. Das Produkt gibt eine Information über die Qualität des Programmcodes und die genutzten Kryptobibliotheken. In dem it's OWL Transferprojekt haben das Fraunhofer IEM und die achelos GmbH vier Monate gemeinsam an der Weiterentwicklung von CogniCrypt gearbeitet. Die Ergebnisse sind in Form eines Wissenstransfers und der Integration zusätzlicher Kryptobibliotheken in das Open-Source-Produkt eingeflossen.

Kontinuierlicher Wissenstransfer im Projekt

Die Security-Expertinnen und -Experten von achelos haben das Produkt in den Continuous-Integration-Prozess ihrer Softwareentwicklung integriert und das Werkzeug getestet. achelos konnte ihr tiefes kryptografisches Wissen im Rahmen des Transferprojekts einbringen und so gemeinsam mit dem Fraunhofer IEM zur kontinuierlichen Weiterentwicklung des Produkts beitragen. CogniCrypt ist um neue Regeln erweitert worden, die Fehlimplementierungen anderer Bibliotheken (Bouncy Castle) erkennen und Sicherheitslücken frühzeitig vermeiden. Die Regeln wurden hierbei konform der Technischen Richtlinie 02102-1 des BSI geschrieben.

CogniCrypt macht die Softwareentwicklung sicherer und qualitativ hochwertiger: Die Experten von achelos werden durch CogniCrypt bei Code Reviews zusätzlich unterstützt, denn das Werkzeug erbringt den Nachweis korrekt genutzter Anwendungsschnittstellen (APIs).

„Die Kryptoexpertise von achelos hat uns einen deutlichen Mehrwert bei der Weiterentwicklung von CogniCrypt gebracht", fasst Dr. Johannes Späth, Seniorexperte am Fraunhofer IEM, die erfolgreiche Zusammenarbeit mit achelos zusammen. „Sicherheit und Kryptografie zählen zu unseren Kernkompetenzen, im Transferprojekt mit dem Fraunhofer IEM konnten wir unsere praktische Erfahrung in das hochperformante Werkzeug einbringen", ergänzt Kathrin Asmuth, Geschäftsführende Gesellschafterin der achelos GmbH

Über CogniCrypt

Im Rahmen des Sonderforschungsbereichs CROSSING der Technischen Universität Darmstadt und in Zusammenarbeit mit dem Heinz Nixdorf Institut der Universität Paderborn wurde das Werkzeug CogniCrypt entwickelt. Es erlaubt Unternehmen im Bereich Sicherheit und Kryptografie, sicherheitskritische Fehlbenutzungen kryptografischer Bibliotheken schnell und zuverlässig zu identifizieren und zu beheben sowie außerdem vollautomatisch sicheren Krypto-Integrationscode für verschiedene gängige Nutzungsszenarien zu generieren. Mit Unterstützung des Fraunhofer IEM wurde CogniCrypt bis zur Marktreife weiterentwickelt und lässt sich in die Entwicklungsumgebung Eclipse einbinden.

www.eclipse.org/cognicrypt/

Über die achelos GmbH

achelos ist ein herstellerunabhängiges Softwareentwicklungs- und Beratungshaus mit Sitz in Paderborn. Der 2008 gegründete Technologieexperte bietet branchenübergreifende Lösungen für sicherheitskritische Anwendungsfelder mit Kernkompetenzen in Embedded Development und Subscription Management. Das Unternehmen entwickelt und betreibt hochspezialisierte Produkte, Lösungen und Dienste für den internationalen Markt. achelos bietet eine umfassende Expertise in Entwicklung, Testing as a Service (TaaS) und Zertifizierung.

achelos.de | **IoT.achelos.com**

Über das Fraunhofer IEM

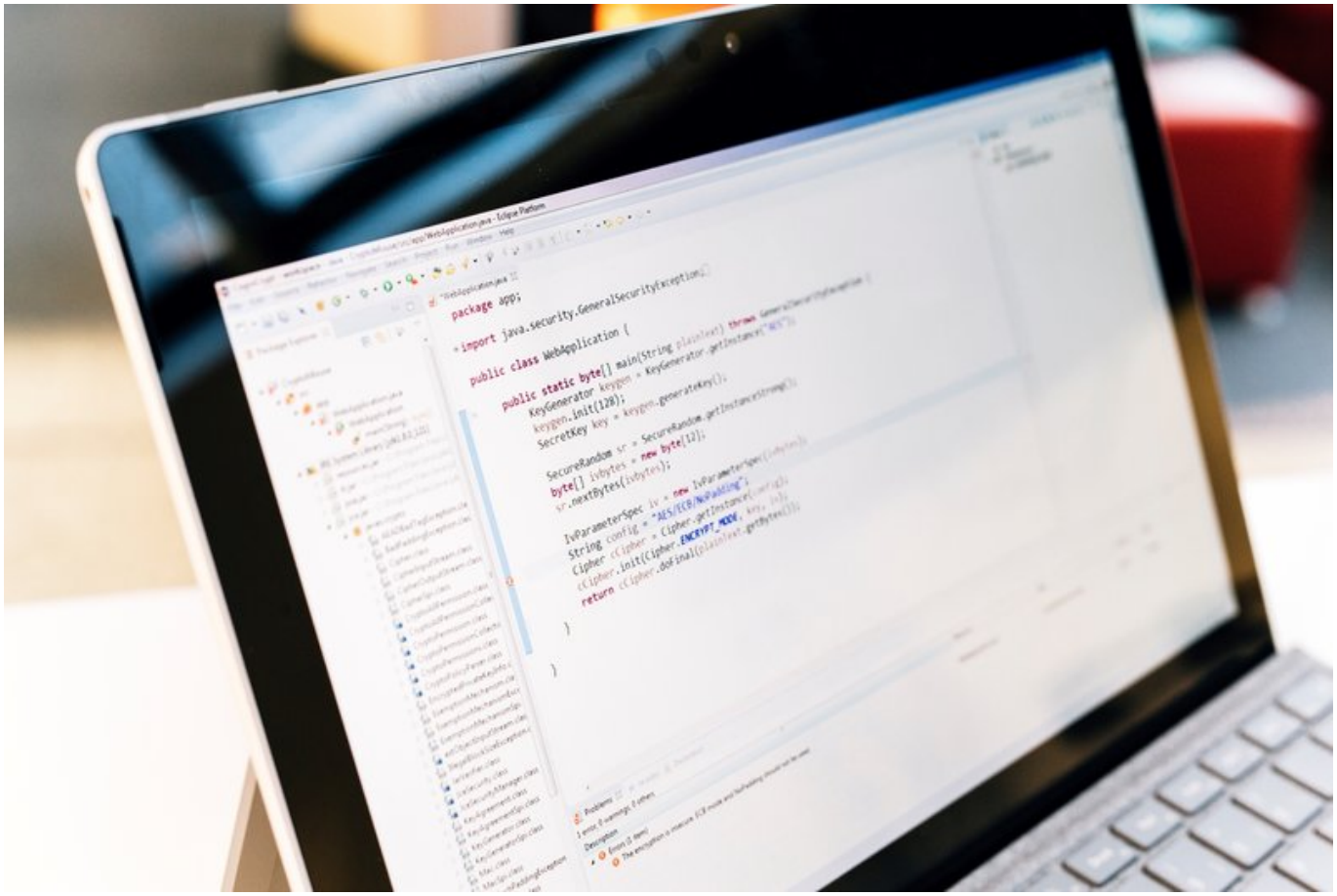
Das Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM bietet am Standort Paderborn Expertise für intelligente Mechatronik im Kontext Industrie 4.0. Wissenschaftlerinnen und Wissenschaftler aus den Bereichen Maschinenbau, Softwaretechnik und Elektrotechnik arbeiten fachübergreifend zusammen und erforschen innovative Methoden und Werkzeuge für die Entwicklung von intelligenten Produkten, Produktionssystemen und Dienstleistungen.

www.iem.fraunhofer.de

Über das Technologie-Netzwerk it’s OWL

Im Technologie-Netzwerk it’s OWL – Intelligente Technische Systeme OstWestfalenLippe entwickeln über 200 Unternehmen, Forschungseinrichtungen und Organisationen Lösungen für intelligente Produkte und Produktionsverfahren. Mit Unterstützung des Landes Nordrhein-Westfalen werden dazu in der Zeit von 2018 bis 2022 Projekte im Umfang von 100 Millionen Euro umgesetzt. Themenschwerpunkte sind künstliche Intelligenz, digitale Plattformen, digitaler Zwilling und Arbeit 4.0. Ausgezeichnet im Spitzencluster-Wettbewerb der Bundesregierung, gilt it’s OWL als eine der größten Initiativen für Industrie 4.0 im Mittelstand.

www.its-owl.de



Das Eclipse-Plug-in CogniCrypt findet Fehlbenutzungen von Kryptografie direkt in der Entwicklungsumgebung. Foto: Fraunhofer IEM