Hagen Buchwald, Vorstandsvorsitzender des Cyber-Forums in Karlsruhe

Anfällige Schnittstellen machen so mancher Software zu schaffen. Die Gefahr ist einfach zu bannen – mit einer 20 Jahre alten Idee

Der Eiffelianer

Schnittstellen sind des Hackers Liebling. Sie nutzen die mangelnde Abstimmung zwischen einzelnen Programmmodulen und dringen so ins System ein. Auch neue Software ist vor solchen Attacken nicht sicher, erklärte Hagen Buchwald, Vorstandsvorsitzender des Cyber-Forums, anlässlich eines Events der Karlsruher IT-Sicherheitsinitiative. „Die Entwicklung krankt daran, dass Schnittstellen zwar syntaktisch präzise beschrieben werden, nicht jedoch in ihrer Semantik. Wie kann ich eine Schnittstelle auf Korrektheit testen, deren Semantik ich nicht vollständig verstanden habe? Bei Tests bleiben wichtige Eigenschaften ungeprüft und werden so zu Schwachstellen, in die Hacker eindringen.“ Prominentes Beispiel: Windows. Auf Herz und Nieren geprüft, dennoch voller Bugs und Sicherheitsrisiken.

Design by Contract (DbC) kann dieses Dilemma lösen. Durch sogenannte Verträge („Contracts“) soll das reibungslose Zusammenspiel zwischen den Modulen besser klappen. „Ein Vertrag sichert den Komponenten Spielregeln zu, die bei der Kommunikation eingehalten werden.“ Das macht den Hackern das Leben schwer, ihre Angriffe werden ignoriert. „Verstöße gegen diese Spielregeln werden bereits in der Implementierungsphase erkannt und abgefangen. Die Robustheit wird durch Tests, die direkt aus den Verträgen abgeleitet werden, überprüft.“

Das Konzept ist nicht neu. Schon als Bertrand Meyer vor mehr als 20 Jahren die Programmiersprache Eiffel entwickelt hat, führte er DbC ein. Das Problem: Eiffel konnte sich damals nicht gegen C++, den Java-Vorgänger durchsetzen. Sie haben die bessere Performance, machen Hackern das Leben aber um einiges leichter. „Die Performance ist ein entscheidendes Qualitätsmerkmal in der IT und dominiert Qualitätskriterien wie Korrektheit oder Robustheit“, sagt Buchwald, der sich selbst als Eiffelianer bezeichnet. Die Konsequenz: Viele Software-Programme sind performant, aber unsicher.

Seit einigen Jahren jedoch arbeiten Informatiker an Zusatzbibliotheken für Java und kombinieren so Schnelligkeit mit der Sicherheit von DbC. Am KIT in Karlsruhe hat Prof. Dr. Ralf Reussner zur Vorhersage der Performance-Eigenschaften großer Software-Systeme das „Palladio Component Model“ entwickelt. „Mit DbC ist ein Qualitätsmanagement in der Software-Entwicklung möglich, das weit über die klassischen Ansätze hinaus geht. Die Schwachstellen werden in der Design-Phase erkannt und in der Entwicklung und analytischen Qualitätssicherung gezielt adressiert.“ Dank Open-Source-Paketen für Java ist dieses Konzept ohne große Vorinvestitionen nutzbar, so Buchwald. „Für viele kleine Software-Firmen ist das ein Segen.“ Für viele Hacker hingegen ist DbC ein Fluch. ***rs***

i

Die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) hat ein neues Mitglied: die Group Business Software AG. Das Unternehmen ist mit seinen Tochtergesellschaften der weltweit größte Anbieter für Softwarelösungen (Applikationen) auf der Plattform IBM Lotus Notes Domino. In Deutschland betreibt Group Standorte in Karlsruhe, Stuttgart, Frankfurt, Karlsruhe, Fulda, Braunschweig, Osnabrück, Stuttgart und Dresden. Stammsitz ist Eisenach. Rund 3000 Kunden mit mehr als drei Millionen Anwendern setzen die Lösungen des Unternehmens ein.

KA-IT-Si
Karlsruher IT-Sicherheitsinitiative

Foto: Jigal Fichtner