PARTNERMELDUNG

Sicheres Cloud Computing statt Software-Crash

15.09.2014

Innsbruck/Wien (PARTNER) - Integration von digitalem Fachwissen und Automatisierung von Risiko-Analysen kann Testverfahren für Software deutlich verbessern und Cloud Computing sicherer machen. Das zeigen neueste Ergebnisse eines Projekts des Wissenschaftsfonds FWF zur Qualitätssicherung sicherheitskritischer Systeme, die soeben veröffentlicht wurden. Die Ergebnisse bilden eine Grundlage für sogenannte nicht-funktionale Sicherheitstests. Diese sollen Schwachstellen von Software identifizieren, die sich nicht aus dem unmittelbaren Programmablauf ergeben - und spielen für Cloud Computing eine immer wichtigere Rolle. Mit den nun entwickelten Grundlagen können solche Tests weiter automatisiert und nutzerfreundlicher gemacht werden.

Software-EntwicklerInnen erleben oftmals böse Überraschungen: Selbst nach langer und erfolgreicher Anwendung von Cloud-Programmen tun sich plötzlich unerwartete Schwachstellen auf. Tatsächlich sind gerade Cloud-Programme anfällig dafür. Nicht weil sie schlecht geschrieben wurden, sondern weil sie viele laufend aktualisierte Schnittstellen besitzen. Diese machen Funktionalitäten erforderlich, die weit über den eigentlichen Programmablauf hinausgehen und von dritten Systemen abhängen. Sogenannte nicht-funktionale Sicherheitstests können diese Aspekte zwar testen, doch die konventionellen Methoden der Qualitätssicherung scheitern oft an der Komplexität der Anforderungen. Jetzt haben WissenschafterInnen der Universität Innsbruck Grundlagen vorgestellt, die nicht-funktionale Tests deutlich verbessern können.

An Besten testen

Die wesentlichen Erfolgskriterien dieser vom Team um Prof. Ruth Breu, Leiterin des Instituts für Informatik, entwickelten Grundlagen sind dabei die Integration von Fachwissen sowie eine Automatisierung der Prozesse zur Risikoanalyse. Die Wichtigkeit für die Integration formalisierten Expertenwissens über Schwachstellen in Software führt die Expertin dabei eindrucksvoll aus: "Allein im Jahr 2012 wurden 9.762 bis dahin unbekannte Sicherheitslücken in der Open Source Vulnerability Database, einer weltweit zugänglichen Datenbank zur Verwaltung von Wissen um Sicherheitslücken in Software, registriert. Tatsächlich sind die Ursachen vieler dieser Sicherheitslücken aber seit Langem bekannt. Sie hätten zum Zeitpunkt der Softwareentwicklung also schon vermieden werden können. Optimierte nicht-funktionale Tests sollten daher auf solches existierendes Wissen zurückzugreifen. Genau das tut unser Verfahren."

Dazu formalisiert das Team um Prof. Breu, Dr. Michael Felderer und Philipp Zech solches Wissen und macht es damit für nachfolgende automatische Risikoanalysen verfügbar. Diese Analysen resultieren in Risikoprofilen der zu testenden Systeme, die zum Erstellen ausführbarer Sicherheitstest verwendet werden. Dabei kommen moderne Programmiersprachen wie Scala und ASP sowie modellbasierte Verfahren zum Einsatz. Zu diesem automatisierten Prozess der Risikoanalyse meint Prof. Breu: "Das Problem bei bisherigen nicht-funktionalen Sicherheitstests ist die schier unendliche Anzahl an Möglichkeiten für Fehler. Bisher versuchte man, diese Situation durch menschliches Expertenwissen zu meistern, z. B. bei Penetrationstests. Die von uns gewählte Herangehensweise erlaubt nun aber ein strukturiertes und automatisiertes Testverfahren."

Praxistest

Prof. Breu ergänzt: "Zunächst war unsere Arbeit ja eher theoretisch geleitet. Doch wir wollten auch die Praxistauglichkeit unserer Überlegungen demonstrieren. Daher haben wir Real-Life Tests durchgeführt, die Reaktionen auf häufige Problemsituationen wie SQL-Injection-Angriffe checken." Im Rahmen der jetzt publizierten Arbeit wurde dabei zunächst auf eigens geschriebene Programme zurückgegriffen. Doch bereits seit einiger Zeit werden vom Team um Prof. Breu auch öffentlich verfügbare Testsysteme verwendet. Mit beeindruckendem Erfolg: Bis zu 90 Prozent aller Schwachstellen können aktuell zuverlässig identifiziert werden.

die zukünftige Qualitätssicherung sicherheitskritischer Systeme dar - ein Ergebnis, das die Bedeutung grundlegender wissenschaftlicher Arbeiten für die reibungslose Funktion unseres Alltages einmal mehr unter Beweis stellt.

Bild und Text ab Montag, 15. September 2014, ab 10.00 Uhr MESZ verfügbar unter:

http://www.fwf.ac.at/de/wissenschaft-konkret/projektvorstellungen/2014/pv201409/

Originalpublikation: P. Zech, M. Felderer, B. Katt and R. Breu: Security Test Generation by Answer Set Programming. The Eighth International Conference on Software Security and Reliability (SERE 2014), IEEE, 2014

Rückfragehinweis:
Prof. Ruth Breu
Universität Innsbruck
Institut für Informatik
Technikerstrasse 21a/2
6020 Innsbruck
T +43 / 512 / 507 - 53200
E ruth.breu@uibk.ac.at

Der Wissenschaftsfonds FWF:
Marc Seumenicht
Haus der Forschung
Sensengasse 1
1090 Wien
T +43 / 1 / 505 67 40 - 8114
E marc.seumenicht@fwf.ac.at

Aussender:
PR&D - Public Relations für Forschung & Bildung Mariannengasse 8
1090 Wien
T +43 / 1 / 505 70 44
E contact@prd.at
W http://www.prd.at