Für sichere Software: Röntgen statt Passkontrolle

Das Softwareanalysewerkzeug JOANA überprüft den Quelltext eines Programms und bietet damit neue Möglichkeiten Sicherheitslücken aufzudecken

Vertrauen ist gut, Kontrolle ist besser – auch bei der Sicherheit von Computerprogrammen. Statt sich auf „Ausweispapiere“ in Form von Zertifikaten zu verlassen, durchleuchtet die neue Softwareanalyse JOANA den Quelltext (Code) eines Programms. Auf diese Weise spürt sie die Lecks auf, über die geheime Informationen nach außen gelangen oder Fremde von außen in das System eindringen können. Gleichzeitig reduziert JOANA die Zahl der Fehlalarme auf ein Minimum. Das am Karlsruher Institut für Technologie (KIT) entwickelte Analysewerkzeug hat sich bereits in realistischen Testszenarien bewährt. Als Nächstes ist eine industrielle Fallstudie geplant.

„Gängige Softwarezertifikate bescheinigen die Vertrauenswürdigkeit des Herstellers. Mit JOANA können wir ergänzend das tatsächliche Verhalten eines Programms überprüfen“, sagt Gregor Snelting, der das Analysewerkzeug mit seiner Forschergruppe am Lehrstuhl Programmierparadigmen des KIT entwickelt hat. Das sei deshalb so wichtig, weil die meisten Schwachstellen auf unbeabsichtigte Programmierfehler zurückgingen. Im Fokus der Wissenschaftler stehen derzeit mobile Anwendungen für Android-Smartphones. Prinzipiell können sie aber fast alle Programme testen, die in den gängigen Sprachen JAVA, C oder C++ geschrieben sind. Zunächst sollen Softwareunternehmen ihre Produkte prüfen lassen können, bevor sie damit an den Markt gehen. Da derzeit noch Fachleute das Einrichten und Bedienen übernehmen müssen, ist JOANA für private Nutzer weniger geeignet.

JOANA überprüft sämtliche Datenkanäle einer Software, durch die Informationen fließen, und findet dadurch die Sicherheitslücken. „Wir unterscheiden zwischen öffentlich sichtbaren Kanälen, die beispielsweise die Nutzeroberfläche abbilden, und geschützten Kanälen, auf die Anwender nicht zugreifen können“, erklärt Snelting. „Für die Sicherheit von geheimen Informationen, wie Passwörtern oder Kontonummern, ist entscheidend, dass sie ausschließlich in geschützten Kanälen befördert werden.“ Wo sich geheime und öffentliche Datenströme kreuzten, sei ein Informationsaustausch prinzipiell

Monika Landgraf
Pressesprecherin

Kaiserstraße 12
76131 Karlsruhe
Tel.: +49 721 608-47414
Fax: +49 721 608-43658
E-Mail: presse@kit.edu

Weiterer Kontakt:

Lilith C. Paul
Presse, Kommunikation und Marketing
Telefon: +49 721 608-48120
Fax: +49 721 608-43658
E-Mail: l.c.paul@kit.edu

möglich und so bestehe Gefahr, dass sensible Informationen weitergegeben würden.

Die Wissenschaftler unterscheiden mehrere Sicherheitslücken: So können beispielsweise direkt lesbare Kopien sensibler Daten nach außen gelangen (explizites Leck) oder nur die Muster, nach denen sie verschlüsselt sind (implizites Leck). Problematisch ist auch, wenn sich geheime Passwörter auf die wahrscheinliche Reihenfolge sichtbarer Informationsflüsse auswirken (probabilistisches Leck) – und daraus rekonstruierbar sind. Ein vereinfachtes Beispiel: Der Befehl ein „rotes L“ zu drucken erreicht einen Drucker zeitgleich mit dem geheimen Passwort für die Zugriffsberechtigung. Lautet das Passwort AB, kommt die Information „L“ in den meisten Fällen kurz vor der Information „rot“ an. Lautet das Passwort BA, ist es genau umgekehrt.. JOANA erkennt auch solche Sicherheitslücken zuverlässig, obwohl sie schwerer zu identifizieren sind.

„Mindestens ebenso wichtig, wie alle Sicherheitslücken zu finden, ist es, möglichst wenig Fehlalarme zu produzieren“, sagt Snelting. Viele Fehlalarme führten zu einem massiv erhöhten Prüfaufwand oder dazu, dass Alarme ignoriert würden. JOANA reduziert die Zahl der Fehlalarme für alle Sicherheitslücken – auch für probabilistische Lecks. Die KIT-Wissenschaftler haben dafür eine neue Rechenmethode entwickelt (Relaxed Low-Security Oberservational Determinism), die nur an sicherheitskritischen Stellen eine feste Reihenfolge für beobachtbare Prozessschritte vorschreibt. Im obigen Beispiel hieße das, die Information „rot“ muss den Drucker immer vor der Information „L“ erreichen, unabhängig vom Passwort. „Die Herausforderung war, sicherheitsirrelevante Prozesse von solch strikten Vorgaben auszunehmen“, so Snelting. Andernfalls stiege entweder die Zahl der Fehlalarme, weil jede Abweichung als gefährlich eingestuft würde, oder die Ausführungen eines Programms müssten so massiv beschränkt werden, dass es praktisch nicht mehr nutzbar sei.

JOANA ist bislang weltweit das einzige Softwareanalysewerkzeug, das nicht nur alle Sicherheitslücken findet, sondern auch die Zahl der Fehlalarme minimiert, ohne die Funktionsfähigkeit von Programmen zu beeinträchtigen. Gefördert von der Deutschen Forschungsgemeinschaft haben die KIT-Wissenschaftler rund zwanzig Jahre auf diesem Gebiet geforscht. „Längerfristig könnte mit JOANA geprüfte Software ein neuartiges Zertifikat erhalten, das die Sicherheit des Programmcodes bescheinigt“, sagt Snelting.

Für interessierte Fachleute steht JOANA als Open Source Software zum Download zur Verfügung: http://pp.ipd.kit.edu/projects/joana

Digitale Pressemappe zum Wissenschaftsjahr 2014

Ob in der Kommunikation, der Energieversorgung oder der Mobilität, in der Industrie, im Gesundheitsbereich oder in der Freizeit: Digitale Technologien sind längst Teil unseres Alltags, sie eröffnen neue Möglichkeiten und bieten Lösungen für gesellschaftliche Probleme. Gleichzeitig stellen sie uns vor Herausforderungen. Chancen und Risiken stehen im Mittelpunkt des Wissenschaftsjahres 2014 – Die Digitale Gesellschaft. Am KIT beschäftigen sich Forscherinnen und Forscher aller Disziplinen mit den vielfältigen – technischen und gesellschaftlichen – Aspekten der Digitalisierung. Kurzporträts, Presseinformationen und Videos dazu bietet die digitale Pressemappe des KIT zum Wissenschaftsjahr:
www.pkm.kit.edu/digitalegesellschaft

Das Karlsruher Institut für Technologie (KIT) ist eine Körperschaft des öffentlichen Rechts nach den Gesetzen des Landes Baden-Württemberg. Es nimmt sowohl die Mission einer Universität als auch die Mission eines nationalen Forschungszentrums in der Helmholtz-Gemeinschaft wahr. Thematische Schwerpunkte der Forschung sind Energie, natürliche und gebaute Umwelt sowie Gesellschaft und Technik, von fundamentalen Fragen bis zur Anwendung. Mit rund 9.400 Mitarbeiterinnen und Mitarbeitern, darunter knapp 6.000 in Wissenschaft und Lehre, sowie 24.000 Studierenden ist das KIT eine der größten Forschungs- und Lehreinrichtungen Europas. Das KIT verfolgt seine Aufgaben im Wissensdreieck Forschung – Lehre – Innovation.

Diese Presseinformation ist im Internet abrufbar unter: www.kit.edu