

Systemfehler: Heimische Computerprofis spüren Bugs auf noch bevor sie entstehen

- Programmierfehler kosten Wirtschaft Milliarden
- Ein verdrehter Buchstabe reicht für Systemkollaps



Österreich hat ein paar Computerwissenschaftler von Weltruf zur Rückkehr bewegen können. Sie arbeiten daran, Fehler in Computersystemen noch vor der Programmierung zu erkennen.

Computerarbeiter mit Windows-Rechner sind gemeinhin recht tolerante Naturen. Erscheint der berüchtigte Bluescreen mit der Fehlermeldung, schimpft der Anwender ein bisschen und drückt „ctrl + alt + reset“ für einen Neustart. Das sind Systemfehler, wie sie jeder Benutzer kennt. Verantwortlich sind falsch programmierte Codezeilen, vom Fachmann „Bugs“ genannt. Das Phänomen gibt es leider auch ein paar Nummern größer: So reichte 1996 ein Bug aus, um die Ariane-5-Rakete vom Himmel zu holen. 1985 „erkannte“ ein Montageroboter bei GM die schwarze Farbe nicht, und diese Autos verließen die Halle ohne Windschutzscheibe. 2003 nahm ein Fehler im Steuerungssystem eines Energieversorgers 50 Millionen Amerikaner und Kanadier bis zu fünf Tage vom Stromnetz.

Solche Bugs kosten Bucks

60 Milliarden Dollar waren es im Jahr 2002 (*Quelle: www.nist.org*), das ist sechsmal so viel, wie Amerikaner für Schönheits-OPs ausgeben. Die Schwachstelle im System ist – praktisch systemimmanent – der Mensch. „Ein falscher Buchstabe in einer Programmzeile reicht aus, um das System zum Kollaps zu bringen“, sagt Computerwissenschaftler Prof. Thomas Henzinger, dessen Forschungsgebiet das Aufspüren von Bugs ist (*rechts im Bild*). Zum Einsatz kommt ein Verfahren, das Model-Checking heißt, übersetzt: Modellprüfung. Vollautomatisiert werden die Varianten des Zusammenspiels der Systeme durchgespielt. Für die Entwicklung dieses Verfahrens stehen drei Computerwissenschaftler: Joseph Sifakis, Edmund M. Clarke und Allen Emerson, die 2007 dafür den „Nobelpreis“ der Informatik, den Turing Award, bekamen.

Griechischer Guru

Joseph Sifakis war diese Woche in Österreich und hielt am Institute of Science and Technology (IST) in Klosterneuburg einen fesselnden Vortrag darüber, wie Programmierer eingebettete Systeme am besten designen. Er ehrte mit seinem Besuch einen verdienstvollen Kollegen und Freund. Henzinger ist eine Koryphäe, gehört in seinem Bereich zu den Wissenschaftlern mit den meisten Zitierungen. Nach 25 Jahren im Ausland, die ihn von der Stanford University über Berkeley und das Max-Planck-Institut bis an die ETH Lausanne führten, rechnete Henzinger eigentlich gar nicht mehr damit, „jemals wieder nach Österreich zurückzukehren“.

Back to the roots

Als Präsident der jungen Forschungsstätte IST Austria ist er seit letztem Herbst mit seinen 47 Jahren der Senior einer Spitzentruppe von heimischen Wissenschaftlern, die auf dem Gebiet der präventiven Fehlersuche in

Computersystemen und im Design von komplizierten Computerprozessen Weltspitze sind. Warum Österreich? „Ehrlich, eine große Portion Glück und Zufall gehört schon dazu“, erzählt Prof. Helmut Veith, der nach Stationen in Pittsburgh, München und Darmstadt an der TU Wien lehrt (*links im Bild*). „Als ich hörte, dass Henzinger zurückkommt, war mir klar, dass es in Österreich sehr spannende Perspektiven gibt.“

Fehler vor dem Entstehen eliminieren

Die wissenschaftliche Perspektive der österreichischen Wissenschaftler trägt den sperrigen Titel „Rigorous Systems Engineering“. Sie versucht noch während des Schreibens der Programmzeilen, a priori, potenzielle Stellen für Kurzschlüsse aufzuzeigen. Also Fehler nicht nur zu finden, sondern von vornherein zu verhindern. Österreich hat nicht nur das Glück, dass ein paar Superhirne sich zur Rückkehr überreden ließen. Um dem frischen Schwung jetzt auch System zu geben, wurde ein Konsortium gegründet – das ARiSE Austrian Rigorous Systems Engineering.

Akademisches Kraftfeld

Neben Tom Henzinger und Krish Chatterjee (IST) sind Helmut Veith, Ulrich Schmid, Uwe Egly und Laura Kovács (TU Wien) dabei. In den Bundesländern sitzen Roderick Bloem (TU Graz), Armin Biere (Uni Linz) und Christoph Kirsch (Uni Salzburg). Diese Mathematiker und Informatiker stellen ein Kraftfeld dar, wie es die heimische Forschungslandschaft seit den Quantenphysikern in Innsbruck und Wien nicht mehr hatte. Neben den Beamern gibt es jetzt Bug-Fixer, eine Elitetruppe für Fehlerbehebung und -vermeidung.

Konkurrierende Softwaresysteme

Eine Spezialität ist die vollautomatische Fehlersuche, Computer Aided Verification genannt. Untersucht werden auch Auswirkungen von eingebetteten Systemen. Nicht einmal zwei Prozent der Prozessoren stecken tatsächlich in PCs. Der große Rest kommt in Autos, Gebäuden, ja sogar Herzschrittmachern zum Einsatz: im Fachjargon „embedded“. Die Computerwissenschaftler unterscheiden bei ihrer Arbeit vielerlei Bugs. Die „concurrency bugs“ treten dann auf, wenn zwei Softwaresysteme zur selben Zeit in Konkurrenz treten. Das ist bereits der Fall, wenn ein Großraumbürodruker gleichzeitig zwei Druckaufträge bekommt. Die zweite Kategorie der „embedded bugs“ betrifft die Fehler zwischen der Software- und der physischen Welt, etwa bei der elektronischen Motorsteuerung im Auto.

10 Milliarden neue Prozessoren

Der fahrbare Untersatz ist ein gutes Beispiel dafür, wie sich diese eingebettete Elektronik in unserer Umwelt verbreitet. Beim Auto haben sich allein in der letzten Dekade die Softwarekosten von 4 auf 13 Prozent erhöht. 35 Prozent der Herstellungskosten gehen beim Auto heute in die Elektronik inklusive Software, haben Forscher des MIT errechnet. „Jedes Jahr kommen zehn Milliarden neue Prozessoren weltweit dazu“, führt Helmut Veith von der TU Wien aus. Die stecken in der Boeing 777 ebenso drin wie im neuen Zimmerthermostat.

Fehlervermeidung bei eingebetteten Systemen

Henzinger erklärt, warum die Fehlervermeidung bei den eingebetteten Systemen so wichtig ist: „Ärger gibt es meist dann, wenn unterschiedliche Systeme zusammenkommen. Ein für sich abgeschlossenes System arbeitet reibungsloser.“ Dass ist mit ein Grund, warum Microsoft traditionell mit mehr Fehlermeldungen leben musste als Apple mit seinem abgeschlossenen Kreislauf. Veith sekundiert: „Oft sind die Programme vom Zweitsystem, also der Treiber von einem Zusatzgerät, schuld am Systemabsturz.“

Teamwork mit der Wirtschaft

Dass die Programme des weltgrößten Softwarebauers Microsoft heute seltener abstürzen, hat damit zu tun, dass Gründer und einst oberster Ingenieur Bill Gates 2002 eine beispiellose Qualitätsoffensive startete. Microsoft investiert viele Millionen Dollar in Rigorous Software Engineering. Die Grenze zwischen Grundlagen- und angewandter Forschung ist hier kaum vorhanden. Henzingers Studenten werden gern in die Forschungsabteilungen von Konzernen abgeworben. Und was machen sie dort? Der Einsatz geeigneter Prüfverfahren kann Hersteller vor großem Schaden bewahren. Bei den Systemen, die in einer Boeing laufen, ist der Test- und Zertifizierungsaufwand für die Software so groß und teuer, dass man eine 2010 ausgelieferte Maschine lieber mit einer geprüften Software von 1995 fliegen lässt. Ein unentdeckter Bug könnte viele Menschenleben kosten.

Schwarzmarkt für Programmfehler

Dass sich selbst Pentagon-Mitarbeiter die Vorträge der Österreicher gern anhören, hat seine Gründe. Für terroristische Angriffe braucht es heute keine Bomben mehr. Es reicht, die Kommunikationslogistik zu stören, um einen Staat tagelang lahmzulegen, wie vor wenigen Jahren Estland. Wie kamen die Hacker ins System? Über Fehler im Programm. „Solche Programmfehler werden auf dem Schwarzmarkt gehandelt“, erzählt Veith, der davon träumt, dass sich dieses Geschäft in einer fehlerfreien Zukunft nicht mehr lohnt.

Barbara Mayerl

Professionelle Fehlersucher. v. l.: Prof. Helmut Veith von der TU Wien, Prof. Roderick Bloem von der TU Graz und Prof. Thomas Henzinger, Präsident der IST Austria, holen die Elite zurück nach Österreich.

6.5.2010 11:11