KI-4-Everyone · Daily News

13. Juli 2026

RES

Microsoft prüft Krypto-Code schon beim Schreiben auf Fehler

Microsoft stellt eine neue Methode vor, die Sicherheitslücken in Kryptografie-Code erkennt, während Entwickler ihn tippen – ohne Geschwindigkeitsverlust.

REG

Apple verklagt OpenAI wegen Diebstahl von Betriebsgeheimnissen

Laut Apples Klage bat OpenAI Bewerber, unveröffentlichte Apple-Hardware zu Vorstellungsgesprächen mitzubringen. Ein Ex-Mitarbeiter soll gezielt eine Sicherheitslücke ausgenutzt haben.

FORSCHUNG

Microsoft laesst Kryptografie-Code beim Schreiben pruefen - direkt in Rust

Ein neuer Ansatz aus der Microsoft-Forschung soll verifizieren, dass kryptografischer Code korrekt ist, ohne dass Entwickler Tempo oder Flexibilitaet verlieren.

Kryptografie ist der unsichtbare Tuersteher der digitalen Welt: Sie schuetzt Passwoerter, Bankgeschaefte, medizinische Daten und Firmengeheimnisse. Doch wenn im Code, der diese Verschluesselung umsetzt, ein winziger Fehler steckt, koennen ganze Sicherheitsarchitekturen einstuerzen. Microsoft Research hat nun einen Ansatz vorgestellt, der genau hier ansetzt - und zwar nicht erst nach der Entwicklung, sondern waehrend Entwicklerinnen und Entwickler den Code schreiben.

Konkret geht es um SymCrypt, die kryptografische Bibliothek, die in vielen Microsoft-Produkten steckt. Teile davon werden inzwischen in Rust geschrieben - einer Programmiersprache, die als besonders sicher gilt, weil sie bestimmte Fehlerklassen von vornherein ausschliesst. In einem am 13. Juli 2026 veroeffentlichten Beitrag beschreibt Microsoft Research eine Methode, wie sich Rust-Code fuer Kryptografie formal verifizieren laesst: also mathematisch beweisen, dass er sich exakt so verhaelt, wie es die zugrundeliegenden Standards vorschreiben. Der Anspruch ist, diesen Nachweis nicht als aufwendigen Zusatzschritt zu fuehren, sondern eingebettet in den normalen Entwicklungsprozess - und dabei Geschwindigkeit und Anpassbarkeit des Codes zu erhalten.

Der Kontext ist wichtig: Kryptografie-Bibliotheken werden staendig weiterentwickelt, etwa weil neue Angriffe bekannt werden oder weil sich Standards aendern - Stichwort Post-Quanten-Kryptografie, also Verschluesselung, die auch kuenftigen Quantencomputern standhalten soll. Bisher galt formale Verifikation (der mathematische Beweis von Programmkorrektheit) oft als etwas, das Projekte ausbremst: Man verifiziert einmal muehsam, danach traut sich kaum jemand, noch etwas zu aendern. Microsofts Ansatz zielt darauf, diesen Zielkonflikt aufzuloesen - Sicherheit auf Beweis-Niveau, aber ohne den Code einzufrieren. Fuer Unternehmen, die auf SymCrypt aufbauen, koennte das bedeuten, dass sicherheitskritische Aenderungen schneller und mit hoeherem Vertrauen ausgerollt werden. Und fuer das Rust-Oekosystem insgesamt ist es ein Signal, dass die Sprache nicht nur fuer Systemprogrammierung, sondern auch fuer beweisbar korrekte Sicherheitskomponenten taugt.

Vieles bleibt allerdings offen. Der Blogbeitrag beschreibt den Ansatz, aber wie breit er innerhalb von SymCrypt schon eingesetzt wird, wie hoch der Mehraufwand fuer Entwickler tatsaechlich ist und ob externe Sicherheitsforscher die Methode unabhaengig geprueft haben, geht aus dem Material nicht hervor. Auch ist unklar, welche Teile der Bibliothek konkret abgedeckt sind und welche nicht - Kryptografie-Code hat oft handoptimierte Passagen, die sich formaler Verifikation traditionell entziehen. Wer die Sache ernst nimmt, sollte auf die technischen Detailveroeffentlichungen warten, in denen typischerweise Grenzen und ungeloeste Faelle stehen.

In den naechsten Wochen lohnt der Blick darauf, ob Microsoft konkrete Zahlen nachliefert - etwa zur Performance im Vergleich zu unverifizierter Rust- oder C-Kryptografie - und ob andere grosse Anbieter aehnliche Wege einschlagen. Denn wenn 'verifizierte Kryptografie waehrend des Schreibens' zum neuen Standard wird, verschiebt sich die Messlatte fuer alle, die sicherheitskritische Software ausliefern.

MARKT

Metas KI-Rechenzentrum könnte über 250 Milliarden Dollar kosten

Meta plant mit dem Hyperion-Campus das teuerste Rechenzentrum der Welt. Laut Bloomberg könnte es mehr als 250 Milliarden US-Dollar verschlingen. Das hätte laut dem Bericht sowohl positive als auch negative Folgen für die betroffene Region.

MARKT

S&P stuft Oracle wegen KI-Investitionen fast auf Ramschniveau ab

Oracle steht nach einer Herabstufung durch S&P Global nur noch eine Stufe vor dem spekulativen Bereich. Grund sind massive KI-Investitionen des Konzerns. Das Rating liegt nun bei BBB-.

SAFE

Anthropics neue KI-Forschung: Was sie zeigt – und was nicht

Anthropic gilt laut MIT Technology Review als wertvollstes KI-Unternehmen der Welt mit einem Wert von knapp einer Billion Dollar. Das Unternehmen forscht unter anderem dazu, ob KI-Modelle Schmerz empfinden können. Was die neueste Entdeckung wirklich bedeutet, bleibt laut dem Bericht begrenzt.

PROD

Waze bekommt Gemini-Integration für persönlichere Routen

Google baut seinen KI-Assistenten Gemini in die Navigations-App Waze ein. Von vier neuen Updates nutzen laut Waze zwei direkt Gemini. Ziel ist es, Trips für Nutzer persönlicher zu gestalten.

RES

KI komponiert Musik: Matthias Röder über die Zukunft des Komponierens

Musikwissenschaftler Matthias Röder stellte einst eine Beethoven-Sinfonie mithilfe von KI fertig. Im Interview mit Heise spricht er darüber, was er für die Zukunft von KI in der Musik erwartet. Das Thema KI-Agenten, die selbst komponieren, steht dabei im Mittelpunkt.

SAFE

HN-Diskussion: Sollen KI-Artikel auf Hacker News markiert werden?

Auf Hacker News fragt ein Nutzer, ob KI-generierte Artikel künftig mit einem eigenen Flag gekennzeichnet werden sollten. Die Markierung soll kein Ranking-Nachteil sein, sondern nur als Hinweis dienen. Offen bleibt, ob das normale Abstimmsystem nicht ausreicht.

PROD

PayPal startet komplett neue App-Oberfläche für Deutschland

PayPal-Nutzer in Deutschland müssen sich an eine vollständig neue Menüführung gewöhnen. Hintergrund ist laut Golem der Rauswurf von PayPal aus Google Wallet. Geduld ist laut dem Bericht gefragt.

PROD

De'Longhi Kaffeevollautomat bei Amazon zum Jahrestiefpreis für 269 Euro

Der De'Longhi Magnifica S ist laut Golem aktuell bei Amazon für 269 Euro erhältlich – das entspricht dem Jahrestiefpreis. Es handelt sich um eine bezahlte Anzeige. Ein KI-Bezug ist in diesem Cluster nicht im Material.