Kampf gegen Zombies in den Prozessoren

Sicherheitslücken am Computer sind vor diesen TU-Forschern nicht sicher: Grazer Team deckte jetzt erneut Schwachstellen auf.

Von Christian Penz

In London ließen gestern drei Forscher der TU Graz aufhorchen: Bei einer hochrangig besetzten Konferenz im Bereich Computersicherheit präsentierten Daniel Gruss, Moritz Lipp und Michael Schwarz gravierende Lücken in der Architektur von Intel-Prozessoren. Zur Einordnung: Es handelt sich um eine Lücke, die weltweit Millionen von Mikroprozessoren betrifft. Und es ist nicht das erste Mal, dass die Grazer fündig wurden.

Blicken wir auf das Vorjahr zurück: Mit ihren Angriffsmethoden namens „Meltdown" und „Spectre" deckten Gruss, Lipp und Schwarz zwei Schwachstellen in den Mikroprozessoren auf. Erst ein Update bewahrte Nutzer davor, dass ihre Daten (auch auf Smartphones) in Gefahr gerieten.

Im heurigen Jänner hat das Forscher-Trio zwei weitere Lücken in der Architektur von Intel-Prozessoren (Baujahr 2012 bis 2018) aufgespürt. Die Namen: „ZombieLoad" und „Store-to-Leak Forwarding" (siehe Info). Diese Sicherheitslücke nutzt die optimierte Arbeitsweise von Computerprozessoren aus, um auf sensible Daten zugreifen zu können. Nachdem die Grazer dies aufdeckten, reagierte Intel mit einem Update.

Neuere Prozessoren galten gegen diese Art von Attacken eigentlich als gesichert, das versicherte auch Intel selbst. Wie die Forscher aber im April herausfanden, kann mit einer minimal veränderten Variante des Angriffscodes auch auf diese zugegriffen werden. Selbst ein Software-Update bot nicht ausreichend Schutz.

Warum die Forschungsergebnisse erst jetzt, Monate nach der Entdeckung, publik gemacht werden, hat einen einfachen Grund: „Wir veröffentlichen sie erst jetzt, weil Intel die Zeit benötigte, um eine Gegenstrategie zu entwickeln", betonte Gruss gestern. Er rät zugleich allen Anwendern, alle neuen, empfohlenen Sicherheitsupdates zu installieren.

Erfolgsteam: Michael Schwarz, Moritz Lipp und Daniel Gruss (v. li.) TUGRAZ

Lexikon der Sicherheitslücken

ZombieLoad: Um schneller arbeiten zu können, bereiten Computersysteme mehrere Arbeitsschritte parallel vor und verwerfen dann jene wieder, die entweder nicht gebraucht werden oder für die es keine Zugriffsrechte gibt. In einem kurzen Moment zwischen Befehl und Check der Zugriffsrechte können die bereits geladenen sensiblen Daten gesehen werden.

Store-to-Leak Forwarding: Dabei wird die optimierte Arbeitsweise von Computerprozessoren ausgenutzt, vorab geladene Daten werden ausgelesen.