idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Universität Duisburg-Essen
Dr. Thomas Wittek
15.07.2022
http://idw-online.de/de/news798520

Forschungsergebnisse
Informationstechnik
überregional

Fingerabdrucksensoren und Krypto-Wallets: Sicherheitslücken entdeckt

Sicherheitsexperten des Softwaretechnik-Instituts paluno an der Universität Duisburg-Essen (UDE) haben eine neue Technik entwickelt, die erstmals das Fuzz-Testing von besonders geschützten Speicherbereichen moderner Prozessoren ermöglicht. Mithilfe dieser Methode haben sie jetzt eine Reihe von Schwachstellen in sicherheitskritischen Programmen entdeckt. Gefördert wurde die Forschung im Rahmen des Exzellenzclusters CASA*.

Sie sollen besonders sensible Daten vor Missbrauch schützen – die „Software Guard Extensions“ (SGX) von Intel. Die weit verbreitete Technologie wird eingesetzt, um einen bestimmten Speicherbereich vom Rest eines Computers abzuschirmen. In einer solchen Enklave lässt sich beispielsweise ein Passwortmanager sicher ausführen, selbst wenn das übrige System von Schadsoftware befallen sein sollte.

Nicht selten schleichen sich allerdings Fehler bei der Programmierung der Enklaven ein. Bereits 2020 hat das paluno-Team um Prof. Dr. Lucas Davi mehrere Schwachstellen in SGX-Enklaven entdeckt und veröffentlicht. Nun ist den Forschern gemeinsam mit Partnern des Exzellenzclusters CASA ein weiterer Durchbruch bei der Analyse-Technik gelungen: Während sie zuvor den Enklaven-Code auf Basis symbolischer Ausführung analysierten, ermöglicht ihre neueste Entwicklung das sehr viel effektivere Fuzz-Testing. Hierbei wird ein Programm mit einer großen Anzahl von Eingaben konfrontiert, um Rückschlüsse auf die Struktur des Codes zu ziehen.

„Fuzzing lässt sich nicht ohne Weiteres auf Enklaven anwenden – schließlich ist deren Speicherbereich ja extra vor Zugriffen von außen geschützt“, erklärt paluno-Wissenschaftler Tobias Cloosters die Herausforderung. „Außerdem sind für das Fuzzing verzweigte Datenstrukturen notwendig, welche wir dynamisch aus dem Enklaven-Code rekonstruieren.“ Forschungspartner Johannes Willbold aus dem Forschungskolleg ‚SecHuman – Sicherheit für Menschen im Cyberspace‘ von der Ruhr-Universität Bochum ergänzt: „Auf diese Weise lassen sich die abgeschirmten Bereiche ohne Zugriff auf den Quellcode analysieren.“

Dank moderner Fuzzing-Technik konnten die Forscher viele, bisher unbekannte Sicherheitslücken aufspüren. Betroffen waren diesmal alle getesteten Fingerabdruck-Treiber sowie Wallets zur Aufbewahrung von Kryptowährung. Hacker könnten diese Schwachstellen ausnutzen, um biometrische Daten auszulesen oder das gesamte Guthaben der gespeicherten Krypto-Währung zu stehlen. Alle Hersteller wurden informiert. Drei Schwachstellen wurden in das allgemein zugängliche CVE-Verzeichnis** aufgenommen.

* Das Exzellenzcluster CASA (Cyber-Sicherheit im Zeitalter großskaliger Angreifer) wird von der Deutschen Forschungsgemeinschaft (DFG) seit 2019 gefördert und ist am Horst Görtz Institut für IT-Sicherheit (HGI) an der Ruhr-Universität Bochum angesiedelt ist.

**CVE steht für Common Vulnerabilities and Exposures und listet größere, öffentlich bekannte Sicherheitslücken. Die hier referenzierten Schwachstellen haben die CVE-Einträge CVE-2021-3675 (Synaptics Fingerprint Driver), CVE-2021-36218 (SKALE sgxwallet) und CVE-2021-36219 (SKALE sgxwallet)

Redaktion: Birgit Kremer, Paluno, Tel. 201/18 3-4655, birgit.kremer@paluno.uni-due.de

wissenschaftliche Ansprechpartner:
Prof. Dr. Lucas Davi, Informatik, Tel. 0201/18 3-6445, lucas.davi@uni-due.de