idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Technische Universität Darmstadt
Claudia Staub

27.02.2023
http://idw-online.de/de/news809905

Forschungsergebnisse, Wissenschaftliche Publikationen
Informationstechnik
überregional

Forschungsteam der TU Darmstadt umgeht Chip-Schutzmechanismen mit neuartigen Glitching-Angriffen

Wissenschaftlerinnen und Wissenschaftler am System Security Lab der TU Darmstadt haben neuartige Glitching-Angriffe auf eingebetteten Prozessoren mit Sicherheitserweiterungen ausgeführt und damit die Schutzmechanismen der „TrustZone-M“ Chips aushebeln können.

Mit Glitching-Angriffen dringen Hacker in geschützte Prozessoren ein, indem sie die Ausführung von Maschinenbefehlen unterbrechen beziehungsweise überspringen. TrustZone-M ist eine Sicherheitserweiterung für eingebettete Prozessoren, die eine sichere Umgebung zur Ausführung sicherheitskritischer Programme sowie zur sicheren Speicherung sensitiver Daten bietet. Solche Prozessoren haben viele Anwendungen in Industrie 4.0, Internet of Things (IoT) oder Automotive . Dieser Angriff erlaubt beispielsweise dem Angreifenden sensitive Informationen der Nutzenden wie zum Beispiel kryptographische Schüssel zu stehlen oder diese zu ersetzen und somit potenziell auf Nutzergeräte oder Fahrzeuge zuzugreifen oder diese zu steuern.

Das Ziel der Glitching-Angriffe ist es, gezielt die Berechnungen des Prozessors zu manipulieren. Die Angriffe können unterschiedlich realisiert werden, beispielsweise mittels Laserstrahlbeschuss, gezielter Änderung des Prozessortaktes oder der Spannungszufuhr des Prozessors. Das Forschungsteam um Professor Ahmad-Reza Sadeghi hat sich aus Kostengründen und Gründen der Genauigkeit für Letzteres entschieden. Dabei wird die Stromzufuhr des Chips gezielt gestört, um Fehler in den Berechnungsausführungen des Chips zu verursachen, die zu einem gezielten Fehlverhalten führen, wie beispielweise unautorisierten Zugang zu sensiblen Daten erlauben. Einige Hersteller wie etwa NXP haben bereits Gegenmaßnahmen in entsprechende Prozessoren eingebaut.

Genau hier hakte das Forschungsteam nach. Sein Ziel war vor allem, jene Absicherungen gegen Glitching-Angriffe zu umgehen und auf geschützte Speicherbereiche entsprechender Prozessoren zuzugreifen. Insgesamt konnten im Praxistest mehrere Chips mit TrustZone-M kompromittiert werden (STM 32L5 und Atmel SAML11) sowie Chips mit zusätzlichen, weitreichenden Gegenmaßnahmen gegen Glitching (LPC55S69 und RT6600 von NXP).

Das Forschungsteam musste dabei mehrere Herausforderungen überwinden. Insbesondere musste der einfache Glitching-Angriff zu einem sogenannten Mehrfach-Glitching-Angriff erweitert werden, da das einfache Glitching die Schutzmechanismen, wie die von z.B. NXPs Chips, nicht überwinden kann. Während es für einfache Spannungs-Glitching-Angriffe bereits kommerzielle Werkzeuge gibt, ist dies für koordinierte, mehrfache Spannungs-Glitching-Angriffe nicht der Fall. Das Team entwickelte daher einen neuartigen Multi-Glitcher.

Suchen und Angreifen

Um koordinierte Multi-Glitching-Angriffe durchzuführen, wurde der Multi-Glitcher auf einer handelsüblichen Entwicklungsplattform implementiert. So ist es möglich, mit nur einem synchronisierenden „Trigger Signal“ mehrere koordinierte und parametrisierte Glitches auszuführen sowie die dafür notwendigen Parameter in kurzer Zeit zu finden.

Der Angriff inklusive Parametersuche dauerte im Durchschnitt einen halben Tag, bis auf den sicheren Speicherbereich zugegriffen werden konnte. Neben dem Angriff wird das Forschungsteam auch mögliche Software- sowie Hardware-basierte Gegenmaßnahmen vorstellen.

Die Arbeit wird auf dem kommenden renommierten „32nd USENIX Security Symposium“ im August 2023 unter dem Titel „Oops ...! I Glitched It Again! How to Multi-Glitch the Glitching-Protections on ARM TrustZone-M” vorgestellt.

Eine Vorabversion ist einsehbar auf Arxiv: https://arxiv.org/abs/2302.06932

Über die TU Darmstadt
Die TU Darmstadt zählt zu den führenden Technischen Universitäten in Deutschland und steht für exzellente und relevante Wissenschaft. Globale Transformationen – von der Energiewende über Industrie 4.0 bis zur Künstlichen Intelligenz – gestaltet die TU Darmstadt durch herausragende Erkenntnisse und zukunftsweisende Studienangebote entscheidend mit.
Ihre Spitzenforschung bündelt die TU Darmstadt in drei Feldern: Energy and Environment, Information and Intelligence, Matter and Materials. Ihre problemzentrierte Interdisziplinarität und der produktive Austausch mit Gesellschaft, Wirtschaft und Politik erzeugen Fortschritte für eine weltweit nachhaltige Entwicklung.
Seit ihrer Gründung 1877 zählt die TU Darmstadt zu den am stärksten international geprägten Universitäten in Deutschland; als Europäische Technische Universität baut sie in der Allianz Unite! einen transeuropäischen Campus auf. Mit ihren Partnern der Rhein-Main-Universitäten – der Goethe-Universität Frankfurt und der Johannes Gutenberg-Universität Mainz – entwickelt sie die Metropolregion Frankfurt-Rhein-Main als global attraktiven Wissenschaftsraum weiter.
www.tu-darmstadt.de

wissenschaftliche Ansprechpartner:

TU Darmstadt
Professor Ahmad-Reza Sadeghi, Leiter des System Security Lab, TU Darmstadt
ahmad.sadeghi@trust.tu-darmstadt.de

Originalpublikation:

Marvin Saß, Richard Mitev, Ahmad-Reza Sadeghi: "Oops..! I Glitched It Again! How to Multi-Glitch the Glitching-Protections on ARM TrustZone-M"
Arxiv: https://arxiv.org/abs/2302.06932
DOI: https://doi.org/10.48550/arXiv.2302.06932