idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Karlsruher Institut für Technologie
Monika Landgraf

21.05.2019
http://idw-online.de/de/news716086

Forschungsergebnisse
Informationstechnik
überregional

Schwachstelle von Clouddienst-Hardware aufgedeckt

Sie sind die Legosteine der Computerhersteller: Field-Programmable Gate Arrays (FPGAs) sind elektronische Bauteile, die sich anders als gewöhnliche Computerchips sehr flexibel einsetzen lassen. FPGAs kommen auch in großen Rechenzentren zum Einsatz, die für Clouddienste genutzt werden, wie sie unter anderem große Tech-Firmen anbieten. Bislang galt die Nutzung solcher Dienste als relativ sicher. Forscherinnen und Forscher des Karlsruher Instituts für Technologie (KIT) haben potenzielle Einfallstore für Cyberkriminelle gefunden, wie sie im Fachjournal IACR erklären. (DOI: 10.13154)

Während herkömmliche Chips meist nur eine sehr spezielle gleichbleibende Aufgabe erfüllen, können FPGAs nahezu jede Funktion beliebiger anderer Chips annehmen, weshalb sie oft bei der Entwicklung neuer Geräte oder Systeme verwendet werden. „FPGAs werden zum Beispiel in der ersten Produktcharge neuer Geräte verbaut, weil man sie im Gegensatz zu einem Spezialchip, dessen teure Entwicklung sich nur bei sehr großen Stückzahlen lohnt, nachträglich noch verändern kann“, sagt Dennis Gnad vom Institut für Technische Informatik (ITEC) des KIT. Man könne sich das etwa so vorstellen, als baue man eine Skulptur aus wiederverwendbaren Legosteinen, statt aus abbindender Modelliermasse, erklärt der Informatiker.

So kommen die digitalen Tausendsassas in unterschiedlichsten Bereichen wie Smartphones, Netzwerken, Internet, Medizintechnik, Fahrzeugelektronik oder Luft- und Raumfahrt zum Einsatz. Dabei verbrauchen FPGAs vergleichsweise wenig Strom, was für die Anwendung in den Serverfarmen von Clouddiensten ideal ist. Daneben haben die programmierbaren Chips noch einen anderen Vorteil: Sie können beliebig aufgeteilt werden. „So kann ein Kunde etwa die obere Hälfte des FPGAs nutzen, ein zweiter die untere“, sagt Jonas Krautter, ebenfalls vom ITEC. Für die Clouddienste ist dies ein attraktives Nutzungsszenario. Dabei geht es zum Beispiel um Aufgaben in den Feldern Datenbanken, KI-Anwendungen wie Maschinelles Lernen oder auch Finanzapplikationen.

Verwendung durch mehrere Nutzer ermöglicht Angriffe

Das Problem: „Die Verwendung eines Chips mit FPGA durch mehrere Nutzer zur gleichen Zeit ist ein Einfallstor für bösartige Angriffe“, sagt Gnad. Trickreichen Hackern nämlich bietet gerade die Vielseitigkeit der FPGAs die Möglichkeit, sogenannte Seitenkanal-Attacken durchzuführen. Dabei ziehen die Angreifer aus dem Energieverbrauch des Chips Informationen, mit denen sie seine Verschlüsselung knacken können. Durch solche chip-internen Messungen könne ein Kunde des Clouddienstes einen anderen ausspionieren, warnt Gnad. Darüber hinaus könnten Hacker verräterische Schwankungen im Stromverbrauch nicht nur ausspähen, sondern auch selbst erzeugen. „So können die Berechnungen anderer Kundinnen und Kunden verfälscht oder sogar der gesamte Chip zum Absturz gebracht werden, wodurch Daten verloren gehen könnten“, erklärt Krautter. Ähnliche Gefahren gebe es auch bei anderen Chips, so Gnad weiter. Etwa solchen, die häufig in Internet-der-Dinge-Anwendungen wie zum Beispiel intelligenten Heizungssteuerungen oder Beleuchtungen eingesetzt werden.

Gnad und Krautter wollen das Problem lösen, indem sie den unmittelbaren Zugriff der Nutzerinnen und Nutzer auf die FPGAs beschränken. „Die Schwierigkeit dabei liegt darin, bösartige Nutzer herauszufiltern ohne gutwillige Verwender zu sehr einzuschränken“, sagt Gnad.

Die Fachveröffentlichung bei IACR:

Gnad, D., Krautter, J., & Tahoori, M. (2019). Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(3), 305-339. https://doi.org/10.13154/tches.v2019.i3.305-339

Weitere Materialien:

Podcast: „FPGA Seitenkanäle“, http://modellansatz.de/fpga-seitenkanaele

Details zum KIT-Zentrum Information · Systeme · Technologien (in englischer Sprache): http://www.kcist.kit.edu

Bildunterschrift: Field-Programmable Gate Arrays (FPGAs) sind flexibler als gewöhnliche, spezialisierte Computerchips. Dazu galten sie bislang als besonders sicher. (Foto: Gnad, KIT)

Weiterer Kontakt:

Kosta Schinarakis, Redakteur/Pressereferent, Tel.: +49 721 608-21165, E-Mail: schinarakis@kit.edu

Dr. Felix Mescoli, Redakteur/Pressereferent, Tel.: +49 721 608 21171, E-Mail: felix.mescoli@kit.edu

Diese Presseinformation ist im Internet abrufbar unter: http://www.sek.kit.edu/presse.php

wissenschaftliche Ansprechpartner:

Kosta Schinarakis, Redakteur/Pressereferent, Tel.: +49 721 608-21165, E-Mail: schinarakis@kit.edu

Dr. Felix Mescoli, Redakteur/Pressereferent, Tel.: +49 721 608 21171, E-Mail: felix.mescoli@kit.edu

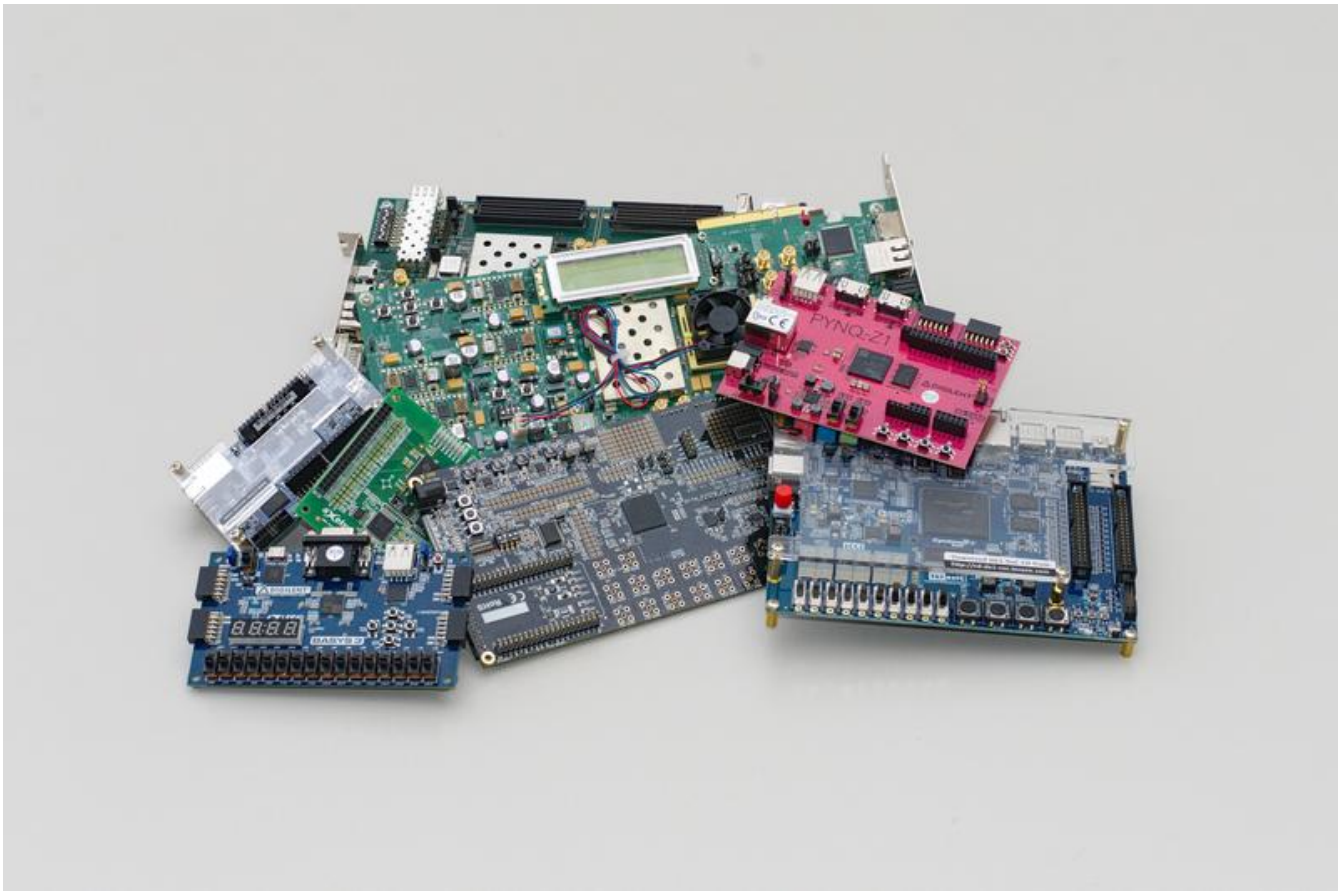
Originalpublikation:

Die Fachveröffentlichung bei IACR:

Gnad, D., Krautter, J., & Tahoori, M. (2019). Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(3), 305-339. https://doi.org/10.13154/tches.v2019.i3.305-339

URL zur Pressemitteilung: http://www.sek.kit.edu/presse.php
URL zur Pressemitteilung: http://felix.mescoli@kit.edu
URL zur Pressemitteilung: http://schinarakis@kit.edu
URL zur Pressemitteilung: http://www.kcist.kit.edu
URL zur Pressemitteilung: http://modellansatz.de/fpga-seitenkanaele
URL zur Pressemitteilung: https://doi.org/10.13154/tches.v2019.i3.305-339

Anhang KIT: Schwachstelle von Clouddienst-Hardware aufgedeckt http://idw-online.de/de/attachment71993



Field-Programmable Gate Arrays (FPGAs) sind flexibler als gewöhnliche, spezialisierte Computerchips. Dazu galten sie bislang als besonders sicher.
(Foto: Gnad, KIT)