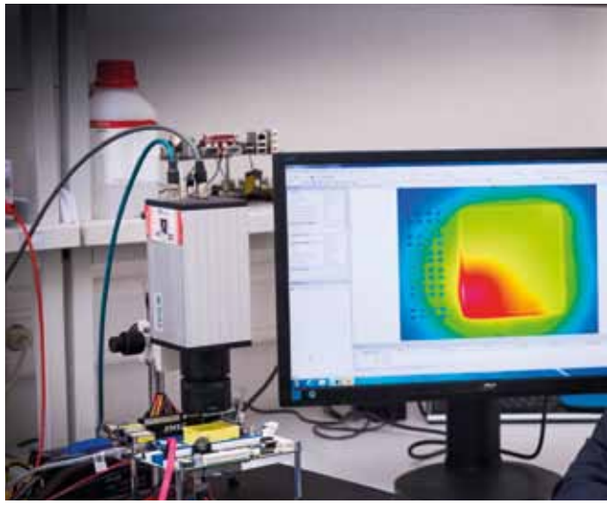
WÄRMEBILDER ZUR ERKENNUNG VON CYBERANGRIFFEN

FOTOS: ANDREA FABRY

WENN CHIPS INS FIEBERN GERATEN

Sicherheitsbedenken lassen viele Unternehmen zögern, wenn es um die konsequente Digitalisierung ihrer Produktionsprozesse im Rahmen von Industrie 4.0 geht. Tatsächlich sind die dafür notwendigen cyber-physikalischen Systeme besonders anfällig für Hackerangriffe. Einem Team am Chair for Embedded Systems des KIT ist jetzt der Nachweis gelungen, dass die Wärmebilder laufender Prozessoren Rückschlüsse auf das Eindringen feindlicher Software zulassen. Unter der Leitung von Professor Jörg Henkel und dem aus dem syrischen Aleppo stammenden Informatiker Dr. Hussam Amrouch entsteht in Zusammenarbeit mit Experten für selbstlernende neuronale Netze an der New York University ein neuartiges Konzept für den Aufbau von Chips, bei denen ein permanentes und sich ständig an neue Bedrohungen anpassendes Selbstüberwachungssystem bereits integriert ist. Für repetitive Steuerungsroutinen digitalisierter Produktionsprozesse sind diese Prozessoren ebenso geeignet wie zur Abwehr ganz neuer Angriffsszenarien, die überhaupt erst durch die fortschreitende Miniaturisierung möglich geworden sind.



lookKIT: In Ihrer Versuchsanordnung registriert eine Infrarotkamera, wie, während der auf dem Chip laufenden Rechenoperationen, unterschiedliche Bereiche des Prozessors kurzzeitig erwärmt werden, um dann wieder abzukühlen. Wie kann man aus diesen rasch ablaufenden thermischen Mustern auf einen Hackerangriff schließen?

Dr. Hussam Amrouch: „Typisch für die cyber-physikalischen Systeme von Industrie 4.0 sind Kontrollschleifen, Wiederholungen eines Programms zur Steuerung eines Produktionsprozesses. Diese Kontrollsequenzen hinterlassen auf dem Chip eine Art thermischen Fingerabdruck. Wenn es gelingt, diesen zu identifizieren, kann man durch Überwachung mit einer Infrarotkamera Abweichungen erkennen. Daraus lässt sich mit hoher Wahrscheinlichkeit schließen, ob jemand eine Malware auf dem Chip laufen lässt. Durch den Vergleich mit dem normalen Abbild des Erwärmungsverlaufs auf dem Chip kann dann ein Sicherheitsalarm ausgelöst werden."

Professor Jörg Henkel: „Wenn man einen Rechner benutzt, geschehen viele unterschiedliche Dinge. Man führt eine Berechnung durch, man speichert etwas im Arbeitsspeicher oder auf der Festplatte. Alle diese Vorgänge erzeugen unterschiedliche thermische Muster auf dem Chip. Wir müssen nun diese Muster in ihrem Verlauf mit einer bestimmten zeitlichen und räumlichen Auflösung beobachten. Da geht es um Millisekunden und minimale Temperaturdifferenzen. Außerdem reden wir zunächst nicht vom PC, der in einem Büro steht, oder vom Handy auf dem unterschiedliche Apps genutzt werden. Im Zusammenhang mit Industrie 4.0 geht es vor allem um genau festgelegte Steuerroutinen im Bereich der industriellen Produktion. Diese ändern sich normalerweise nicht. Falls sie sich einmal ändern, würde man das gesamte System neu aufsetzen. Die Infrarotkamera in unserem Versuchsaufbau dient nur der Forschung. Wenn die Grundlagen einmal geklärt sind, werden Sensoren auf dem Chip ihren Platz einnehmen. Schon heute gibt es Wärmesensoren auf den Chips. Sie dienen dort als Überhitzungsschutz. Wir werden die Zahl der Sensoren vergrößern und sie erstmals zu Zwecken der Cybersecurity einsetzen. Das Ziel ist es, den Chipherstellern genau sagen zu können, wie viele thermische Sensoren man braucht und wo genau sie auf dem Chip angebracht sein sollten, damit sich der thermische Fingerabdruck jeder Rechenoperation zuverlässig erfassen lässt."

lookKIT: Wie wird der thermische Fingerabdruck abgenommen, der für das Monitoring dann die „Normalität" darstellt?

Hussam Amrouch: „In der Forschungsphase speichern wir die Daten und führen die Berechnung des normalen Verhaltens des Chips nachträglich durch. In der Praxis werden neuronale lernfähige Netze integraler Bestandteil des Chipaufbaus sein. Sie werden die Daten der Wärmesensoren im Normalbetrieb in Echtzeit permanent verfolgen. Auf diese Weise erlernen sie, was für diesen Chip zulässig ist und was nicht. Wenn Sie dann irgendwann feststellen, die räumliche und zeitliche Verteilung der Temperaturdifferenzen passt nicht zum gewohnten Bild, können sie Alarm schlagen, dass wahrscheinlich ein unerlaubtes Programm ausgeführt wird."

Jörg Henkel: „Die Lernphase wird nicht nur am Anfang stattfinden. Das Lernen muss kontinuierlich stattfinden. Der Algorithmus, den wir entwickeln, wird ständig weiterlaufen, solange

Dr. Hussam Amrouch vom Chair for Embedded Systems mit einer Aufnahme eines Wärmebildes von Prozessoren (Foto oben)

Dr. Hussam Amrouch from the Chair for Embedded Systems with a thermal image of processors (top)

der Prozessor genutzt wird. Ein Bereich des so veränderten Chips wird für diese Überprüfungen und die ständige Verbesserung seiner Analysefähigkeiten reserviert sein, weil sich die Bedrohung ja auch verändern kann. Irgendwann müssen die Angreifer davon ausgehen, dass es diese permanente Überwachung gibt. Deshalb muss der durch unsere thermische Überwachung geschützte Chip auch modifizierte Strategien erkennen können."

Hussam Amrouch: „Angreifer werden sich anpassen. Wenn sie wissen, dass die Temperatur überwacht wird, werden sie kleinere oder langsamere Programme schreiben, deren Erwärmungsprofile schwerer zu erkennen sind. Dann muss das neuronale Netzwerk in der Lage sein, auch diese geringeren Abweichungen von der Norm zu erkennen. Das kann nur durch eine konstante Verbesserung der Analysefähigkeit des neuronalen Netzwerkes erreicht werden. Das Lernen der Programme wird kontinuierlich angepasst, weil auch die Hacker ständig ihre Methoden ändern."

lookKIT: Mit der exponentiellen Miniaturisierung der Prozessoren bis hin zur Nanoebene sind ganz neue Angriffsszenarien möglich geworden. Man kann durch entsprechende Malware die Hardware selbst angreifen?
Hussam Amrouch: „Früher haben Schaltungen auf den Chips viele Jahrzehnte ohne merkliche Alterung gehalten. Heute sind wir bei der Miniaturisierung in der Größenordnung von 7 Nanometern angelangt. Manchmal wird bereits durch ein paar Elektronen geschaltet. Damit sind Alterungsprozesse kein Langzeitproblem mehr. Was früher Jahre dauert, kann heute schon in einigen Monaten in einen kritischen Zustand geraten. Wir versuchen zu verstehen, wie das von Hackern genutzt werden könnte. Wenn Angreifer heute ein System lahmlegen wollen, können sie innerhalb von Tagen einen künstlichen Alterungsprozess auslösen. Wenn das System dann zu einem kritischen Zeitpunkt gebraucht wird, kann es plötzlich zusammenbrechen. Der Austausch der Chips auf Verdacht ist unter Umständen sehr teuer. Unser technologisches Konzept kann hier sehr wertvoll sein."

Neben seiner Funktion am CES ist Professor Jörg Henkel im Vorstand des Sonderforschungsbereiches/Transregio 89 „InvasIC". Der Transregio 89 ist ein von der Deutschen Forschungsgemeinschaft geförderter Sonderforschungsbereich mit Wissenschaftlern des KIT, der Friedrich-Alexander-Universität Erlangen-Nürnberg sowie der Technischen Universität München. Gemeinsam erforschen sie Invasives Rechnen

Besides his function as CES director, Professor Jörg Henkel is in the board of the Collaborative Research Centre/ Transregio 89 "InvasIC." In this compound structure scientific researchers from KIT, Friedrich-Alexander-Universität Erlangen-Nürnberg, as well as the Technische Universität München conduct research on invasive computing

lookKIT: Kann man sagen, dass Ihr thermisches Überwachungssystem eine Art Gesundheitscheck für Chips darstellt?
Hussam Amrouch: „Wenn man als Mensch Fieber hat, ist die Leistungsfähigkeit ebenfalls herabgesetzt. Auch beim Menschen bedeutet Fieber nur wenige Grad mehr. Das ist beim Chip ähnlich. Ein paar Grad und eine minimale Verlangsamung reichen schon aus, dass man daraus auf einen krankhaften Zustand schließen kann."

Jörg Henkel: „Wir sehen neue Arten der Bedrohungen im Cyberspace, die erst durch den Fortschritt der Technologien möglich wurden. Das Problem der Alterung gab es vor 15 Jahren gar nicht. Eine durch Malware induzierte künstliche Alterung war überhaupt nicht möglich. Technologische Fortschritte wie größere Geschwindigkeiten, kleinere Baugrößen, geringere Kosten haben durchaus unerwünschte Nebenwirkungen. Die gute Nachricht ist, dass die Fortschritte der künstlichen Intelligenz uns heute auch in die Lage versetzen, Chips zu bauen, die auf der Grundlage selbstlernender Algorithmen diese Bedrohungen erkennen und damit abwehren können." ■

Kontakt: henkel@kit.edu, amrouch@kit.edu
Info: ces.itec.kit.edu
Das Gespräch führte Dr. Stefan Fuchs

When Chips have fever

Monitoring Heating Patterns of Cyber Physical Systems Can Detect Cyber Attacks

TRANSLATION: RALF FRIESE

A team of researchers at the Chair for Embedded Systems of KIT headed by Professor Jörg Henkel and Dr. Hussam Amrouch succeeded in demonstrating that thermal patterns produced on the surface of processors in the course of operation can be used to identify attacks by hackers. Temperature fluctuations and their spatial distribution across the chip represent a kind of fingerprint of the proper use of hardware. Deviations from such a thermal fingerprint once detected can be employed as signs of anomalies, perhaps indicative of cyber attacks.

This technique lends itself particularly well to monitor control routines in production processes such as those occurring in connection with Industry 4.0. However, it can also be used for early detection of aging processes in hardware, a growing problem in advanced nanotechnology. Scientists are working on the design of a new generation of processors in which thermal sensors together with machine learning run in the background towards monitoring heating patterns of cyber physical systems and, hence, detecting security attacks. Their use in critical processes will strongly improve IT safety. ■

Contact: henkel@kit.edu, amrouch@kit.edu