Universität Stuttgart

Presseinformation
28.5.2019

Cyberabwehr für die Nanoelektronik

Neues DFG-Schwerpunktprogramm „Nano Security“ an der Universität Stuttgart

Ob Autos, Industrieanlagen oder das Regierungsnetz: Spektakuläre Cyber-Angriffe in den vergangenen Monaten haben gezeigt, wie anfällig elektronische Systeme heute sind. Sie zu schützen und Cyber-Attacken künftig zu verhindern ist das Ziel des neuen Schwerpunktprogramms (SPP) „Nano Security“, das von der Universität Stuttgart koordiniert wird. Das von der Deutschen Forschungsgemeinschaft (DFG) geförderte Programm hebt darauf ab, die Hardware zum vertrauenswürdigen Fundament eines Systems beziehungsweise zum Sicherheitsanker zu machen.

Wirtschaft, Wissenschaft und Gesellschaft sind heute in hohem Maße von elektronischen Systemen abhängig, und schon ein paar gewiefte Hacker können diese knacken – mit katastrophalen Folgen. Doch die Sicherheitsmaßnahmen sind lückenhaft: Die Mehrheit der verfügbaren Cyberabwehrsysteme konzentriert sich auf den Schutz des Softwareteils von elektronischen Systemen oder deren Kommunikationsschnittstellen. Fortschritte in der Fertigungstechnologie sowie die zunehmende Hardwarekomplexität haben jedoch dazu geführt, sich der Fokus der Angreifer zunehmend auch auf die Hardwareebene verlagert. Es mehren sich die Anzeichen für starke und erfolgreiche Angriffe auf Hardware, die mit modernster mikroelektronischer Technologie hergestellt wurde, darunter Sicherheitslücken wie Rowhammer, Meltdown und Spectre.

Herausforderung Nanoelektronik

Völlig neue Herausforderungen stellen sich zudem durch den Umstieg auf radikal neuartige nanoelektronische Komponenten, die zum Beispiel gebraucht werden, um die künftigen Anforderungen in punkto

Hochschulkommunikation

Leiter Hochschulkommunikation und Pressesprecher
Dr. Hans-Herwig Geyer

Kontakt
T 0711 685-82555

Ansprechpartnerin
Andrea Mayer-Grenu

Kontakt
T 0711 685-82176
F 0711 685-82291
hkom@uni-stuttgart.de
www.uni-stuttgart.de

Energieeffizienz, Rechenleistung und sichere Datenübertragung zu bewältigen. Beispielhaft genannt seien Memristoren (Bauteile, die nicht nur zur Informations-Speicherung eingesetzt werden, sondern auch als Logikbausteine fungieren), die Spintronik, bei der man sich quantenmechanische Effekte zunutze macht, oder Kohlenstoff-Nanoröhrchen.

Die neuen Technologien sowie die damit verbundenen grundlegend anderen Computerarchitekturen bieten neue Möglichkeiten für kryptographische Primitive, um eine noch sicherere Datenübertragung zu erreichen. Sie werfen aber auch Fragen nach ihrer Anfälligkeit für neuartige Hardwareangriffe auf.

Problem ist Teil der Lösung

Vor diesem Hintergrund soll im Rahmen des neuen Schwerpunktprogramms ein besseres Verständnis dafür entwickelt werden, welche Folgen die neuen Nanoelektronik-Technologien für die Sicherheit von Schaltungen und Systemen haben. Dabei wird die Hardware nicht nur als Teil des Problems, sondern auch als wichtiger und notwendiger Teil der Lösung von Sicherheitsproblemen aufgefasst. Ansatzpunkte hierfür sind zum Beispiel die hardwarebasierte Erzeugung von kryptografischen Schlüsseln, die sichere Abspeicherung und Verarbeitung von sensitiven Daten oder die durch Hardware garantierte Isolation von Systemteilen. Letzteres soll dafür sorgen, dass ein Angriff sich nicht durch das System weiter verbreiten kann.

Auf dem Weg dahin wollen die Wissenschaftlerinnen und Wissenschaftler mögliche Sicherheitsrisiken und -schwachstellen bewerten, die von der neuartigen Nanoelektronik herrühren. Des Weiteren wollen sie innovative Ansätze für die Systemsicherheit entwickeln, die auf der Nanoelektronik als Sicherheitsanker basieren.

Das SPP fördert Kooperationen zwischen Wissenschaftlerinnen und Wissenschaftlern, die auf verschiedenen Abstraktionsebenen innovative Sicherheitslösungen für Rechensysteme der Zukunft entwickeln. Ebenso soll es Systementwerfern Methoden zur Verfügung stellen, um das Rennen zwischen Angriffen und Schutzmaßnahmen in den nächsten Jahrzehnten für sich zu gewinnen.

Call gestartet

Das DFG-Schwerpunktprogramm „Nano Security. From Nano-Electronics to Secure Systems“ (SPP 2253) ist auf sechs Jahre angelegt. Der Call für die Projekte der ersten, dreijährigen Förderperiode wurde vor wenigen Tagen ausgeschrieben, die ersten Projekte sollen Anfang 2020 starten.

Weitere Informationen (engl.): https://spp-nanosecurity.uni-stuttgart.de/

Fachlicher Kontakt:

Prof. Ilia Polian, Universität Stuttgart, Institut für Technische Informatik,
Tel. +49 711 685 60 764, E-Mail: ilia.polian (at) informatik.uni-stuttgart.de

Pressekontakt:

Andrea Mayer-Grenu, Universität Stuttgart, Hochschulkommunikation,
Tel. +49 (0)711/685 82176,
Mail: andrea.mayer-grenu (at) hkom.uni-stuttgart.de