Adaptive Hardware

für mehr IT-Sicherheit

Hardware, die in ihrer Funktion dynamisch veränderbar ist, ermöglicht heute Lösungen, die mit den bisherigen Mitteln der Informationstechnologie nicht erreicht werden können. Extrem hohe Geschwindigkeiten als auch die Fähigkeit zur nachträglichen Anpassung bieten vielfältige Ansätze für IT-Sicherheitstechnologien. Diese Vorteile können wir für zukünftige Systeme praktisch nutzen.

Adaptable Hardware as a Powerful Means to Improve IT Security

The ability to dynamically change the functionality of hardware modules yields novel technical solutions to many computation problems, which were not achievable before. Inherent high processing speeds as well as the ability to adapt the functionality of a system at any time make this so called reconfiguration technology the premier choice in IT security applications. How can we make use of the unique advantages of adaptable hardware for future systems?

Sorin A. Huss, Andreas Koch, Sascha Mühlbach, Marc Stöttinger • Dank der rasanten Entwicklung der Prozessortechnik in den letzten Jahrzehnten sind wir es gewohnt, dass sich die Leistung von Computern etwa alle zwei Jahre verdoppelt. Allerdings haben technologische Grenzen seit einiger Zeit zu einer Stagnation der Leistung eines einzelnen Prozessors geführt. Ausgeglichen wird dieses Defizit durch die Verwendung von Mehrprozessorsystemen oder durch den Einsatz von speziell für einen Anwendungsbereich zugeschnittener Hardware, die in diesem Bereich deutlich schneller arbeitet als ein generischer Prozessor. Verwendet wird solche Spezialhardware zum Beispiel für die Beschleunigung der Wiedergabe von HD-Videos.

Allerdings ist bei diesem Ansatz für jedes weitere Anwendungsgebiet eine neue spezialisierte Hardware erforderlich, deren Entwicklung und Fertigung sehr aufwendig ist. Eine interessante Alternative sind rekonfigurierbare Hardware- Architekturen, bei denen die Funktionalität der Hardware-Elemente dynamisch umprogrammiert werden kann und nicht bereits durch den Produktionsprozess festgelegt ist. Die am häufigsten verwendete konfigurierbare Architektur ist hierbei das Field Programmable Gate Array (FPGA) (siehe Info-Box).

Andreas Koch

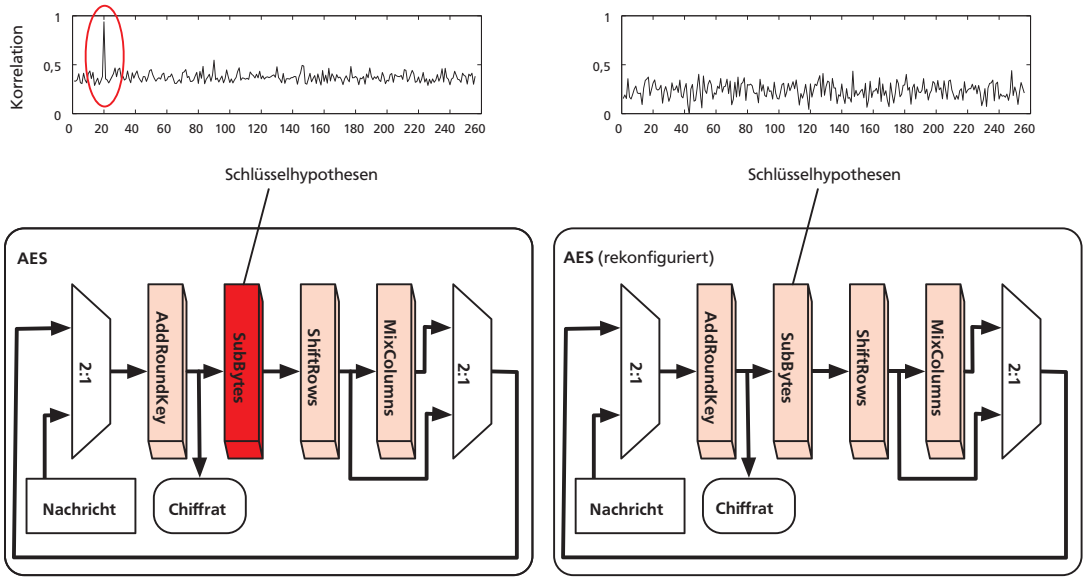


Abbildung 1
Seitenkanalangriffe: Durch Schwachstellen in der Funktion „SubBytes" des Verschlüsselungsverfahrens AES kann ein Angreifer Informationen über den Schlüssel extrahieren. Rekonfigurierbare Hardware kann das verhindern.

Rekonfigurierbare Architekturen erobern zurzeit aufgrund dieser Vorteile eine Reihe von Anwendungsfeldern, insbesondere auch im Bereich der IT-Sicherheit. Durch die wesentlich höhere Leistungsfähigkeit gegenüber rein softwaregestützten Lösungen können selbst moderne Hochgeschwindigkeitsnetzwerke vollständig abgesichert werden. Zudem ist es möglich, auf direkte Angriffe auf die Hardware, wie etwa durch Seitenkanalangriffe, zu reagieren und gefährdete Systeme nachträglich abzusichern. Die folgenden zwei Beispiele aus der Praxis zeigen, wie mittels dieser Tech-

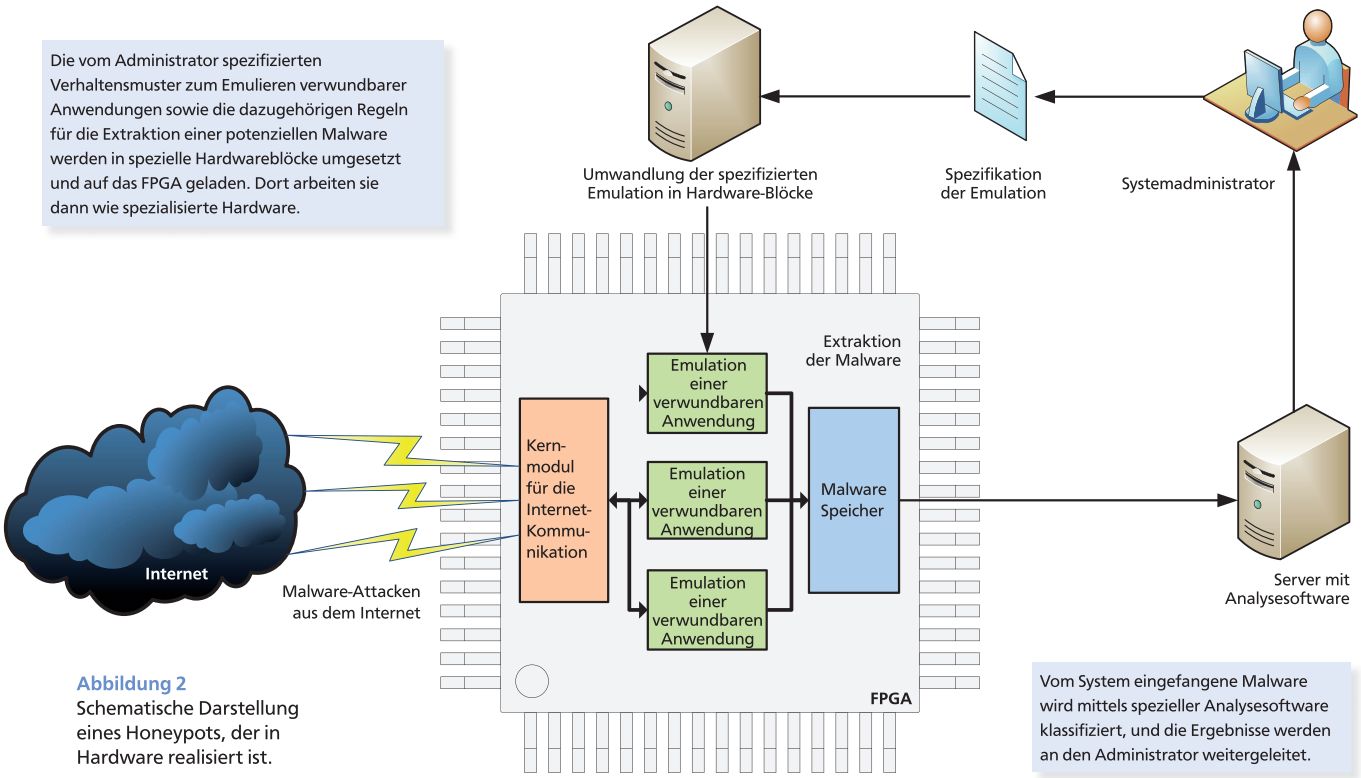


Abbildung 2
Schematische Darstellung eines Honeypots, der in Hardware realisiert ist.

nologie leistungsfähige Plattformen zur Lösung von aktuellen Problemen der IT-Sicherheit geschaffen werden können.

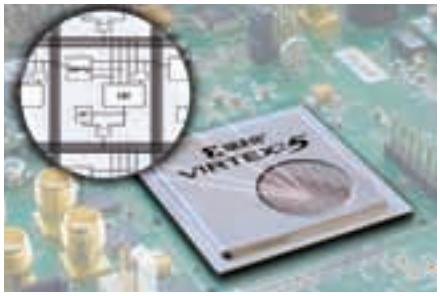
Die Bedrohung durch Schadprogramme, sogenannte Malware, gehört derzeit zu einer der größten Gefahren im Internet. Diese Programme sind oftmals darauf ausgelegt, vertrauliche Informationen zu stehlen oder die Kontrolle über Rechner zu übernehmen. Sie werden über Schwachstellen in Anwendungsprogrammen verbreitet, die zum Beispiel bei der Kommunikation über das Internet ausgenutzt werden.

Virenscanner bieten einen gewissen Schutz vor solchen Bedrohungen, indem sie den Computer regelmäßig nach Verhaltensmustern untersuchen, die auf Schadprogramme hindeuten können. Allerdings entwickelt sich diese Malware kontinuierlich weiter. Es ist daher notwendig, die Erkennungsalgorithmen für bösartige Software ständig zu aktualisieren. Zu diesem Zweck sammeln Wissenschaftler möglichst viele Schadprogramme zur Analyse. Als Quelle hierfür dienen unter anderem spezielle Computersysteme, deren Zweck es ist, automatisch Malware anzulocken. Diese Systeme, sogenannte Honeypots, bilden verwundbare Anwendungsprogramme nach (emulieren sie) und werden ungeschützt im Internet platziert, wo sie von Malware infiziert werden sollen.

Der Aufbau solcher größtenteils ungeschützter Systeme birgt jedoch das Risiko, dass diese selber gekapert und für Angriffe auf weitere Maschinen missbraucht werden können. Zudem wird eine hohe Rechenleistung benötigt, um möglichst viele Angreifer bedienen zu können und so ein breites Spektrum unterschiedlicher Malware zu erhalten. Unter Berücksichtigung dieser beiden Punkte arbeiten Wissenschaftler des Fachgebiets „Eingebettete Systeme und ihre Anwendungen“ am CASED an

FPGA – Field Programmable Gate Array

Ein typisches FPGA besteht aus mehreren zehntausend frei programmierbaren Verarbeitungselementen, den Logikzellen. Diese sind regelmäßig angeordnet und mittels einer flexibel programmierbaren Struktur miteinander verbunden. Jede Zelle enthält ein 2^n Bit großes RAM, in dem alle logischen Funktionen mit n Eingängen realisierbar sind. Die Funktionswerte werden als Look-Up-Wertetabelle abgespeichert.



Zusätzliche Elemente dienen zur Optimierung von häufig auftretenden Operationen, wie etwa der Addition. Zur Konfiguration eines FPGA werden die Look-Up-Tabellen und die Verbindungsstruktur umprogrammiert. Die aktuelle Konfiguration kann dabei jederzeit überschrieben werden.

Sorin A. Huss

einem speziellen Honeypot, der durchgängig in Hardware realisiert ist. Durch die Verwendung von FPGAs können die verschiedenen Anwendungsemulationen flexibel programmiert werden. Trotzdem besteht nicht die Gefahr, dass das System gekapert wird, da Hardware-Strukturen im Gegensatz zu Software von außen nur schwer beeinflussbar sind. Zudem kann durch die Ausnutzung von parallelen Rechenoperationen auf dem Chip eine hohe Anzahl von Anfragen gleichzeitig verarbeitet werden.

Der Kern des Systems, siehe Abbildung 2, ist eine sehr schnelle Implementierung der Basisprotokolle, die für die Kommunikation im Internet benötigt werden. An diese Protokolle sind die einzelnen Emulationen verwundbarer Anwendungen angeschlossen. Eine Emulation ist immer nur für einen bestimmten Typ von Anfrage (z. B. Internet oder E-Mail) zuständig und emuliert die dort gängigen Schwachstellen. Einkommende Anfragen werden vom Kern analysiert und an die dafür zuständige Emulation weitergereicht. Die Funktionalität der Emulationen wird vom Administrator in einer speziellen Beschreibungssprache definiert und automatisch in eine ausführbare Hardware-Einheit umgesetzt. Die dadurch eingefangene Malware wird gespeichert und kann dann zum Beispiel mit Hilfe von Analyseprogrammen weiterverarbeitet werden. Das System hilft somit, sich ausbreitende Malware auch bei der weiter zunehmenden Geschwindigkeit der Datennetze schnell

Fachgebiet Integrierte Schaltungen und Systeme
Prof. Dr.-Ing. Sorin A. Huss
Tel. 06151/16-3980
E-Mail: huss@iss.tu-darmstadt.de, sorin.huss@cased.de

Dipl.-Ing. Marc Stöttinger
Tel. 06151/16-3978
E-Mail: stoettinger@iss.tu-darmstadt.de
www.vlsi.informatik.tu-darmstadt.de
www.cased.de

Fachgebiet Eingebettete Systeme und ihre Anwendungen
Prof. Dr.-Ing. Andreas Koch
Tel. 06151/16-4378
E-Mail: koch@esa.cs.tu-darmstadt.de

Dipl.-Ing. Sascha Mühlbach,
Tel. 06151/16-50182
E-Mail: sascha.muehlbach@cased.de
www.esa.cs.tu-darmstadt.de

zu erkennen und frühzeitig Gegenmaßnahmen zu ergreifen.
Neben Software-gestützten Angriffen auf Computersysteme können heutzutage jedoch auch direkt die Hardware-Komponenten eines Systems Ziel von Angriffen sein und müssen dementsprechend gesichert werden. Eingebettete Systeme, also in sich abgeschlossene Computersysteme in Miniaturformat, breiten sich vermehrt in allen Lebensbereichen aus. Dadurch verarbeiten sie auch immer mehr persönliche und vertrauliche Informationen. Um rechenintensive Sicherheitsfunktionalitäten wie Verschlüsselungsverfahren in diese Systeme zu integrieren, wird spezialisierte Hardware eingesetzt. Diese ist meist schneller und insbesondere stromsparender als eine Software-gestützte Lösung.
Jedoch stellen spezielle Hardware-Angriffsverfahren wie Seitenkanalangriffe eine Gefahr für die privaten Daten in diesen Systemen dar. Seitenkanalangriffe nutzen das Laufzeitverhalten der implementierten Verschlüsselungsverfahren, um daraus Informationen für einen Angriff zu erhalten. Sehr verbreitet sind auf Leistungsanalysen basierende Angriffe (Power Attacks). Dabei misst der Angreifer die Leistungsaufnahme des Geräts im aktiven Zustand, während das Gerät das korrespondierende Chiffrat oder die unverschlüsselte Nachricht verarbeitet. Unter Kenntnis des Verschlüsselungsalgorithmus kann er nun Hypothesen für den im System verwendeten geheimen Teilschlüssel über den datenabhängigen Leistungsverbrauch einer markanten (z. B. leistungsintensiven) Operation im Algorithmus aufstellen. Der Angreifer vergleicht danach die vom Gerät aufgezeichneten Leistungsmessungen mit den Hypothesen durch statistische Methoden. Hierfür wird in der Regel ein Korrelationsverfahren zum Schätzen des Wertes eines Teilschlüssels mit einer hohen Zuverlässigkeit verwendet.
Angreifer können beispielsweise bei dem Verschlüsselungsverfahren AES die Funktion „SubBytes“ ausnutzen, um anhand ihres stark datenabhängigen Leistungsverbrauchs Hypothesen für einen Seitenkanalangriff aufzustellen. Mit Hilfe dieser Hypothesen kann dann mit einem Korrelationsverfahren die wahrscheinlichste Hypothese und damit der richtige Teilschlüssel gefunden werden. (siehe Abbildung 1, links).

Rekonfigurierbare Architekturen bieten hingegen die Möglichkeit, Eigenschaften des Designs nachträglich zu ändern (sollte ein existierendes Gerät anfällig für einen Angriff sein) und sogenannte Verschleierungs- und Maskierungsmaßnahmen in die Schaltung einzubringen. Dies ist einer der Forschungsschwerpunkte der Mitarbeiter im Seitenkanallabor „SCALab“ am CASED.
Bei AES wird dies zum Beispiel durch die Anwendung der Techniken auf die Operation SubBytes oder den gesamten Algorithmus erreicht. Im Ergebnis führt dies zu einem insgesamt niedrigeren und besser balancierten Leistungsverbrauch und erschwert somit den Angriff. Der rechte Teil der Abbildung 1 demonstriert die Auswirkung einer Verschleierungsmaßnahme direkt auf der Funktion SubBytes im Vergleich zum linken Teil.
Im ewigen Wettstreit mit dem Angreifer entwickeln sich sowohl die Angriffe als auch deren Abwehr weiter. Rekonfigurierbare Architekturen bieten hier die Möglichkeit, auch die Hardware (und nicht nur die Software) bestehender Systeme noch nachträglich zu sichern.

Sorin A. Huss ist seit 1990 Professor an der TU Darmstadt und Leiter des Fachgebiets „Integrierte Schaltungen und Systeme“ sowie des CASED-Forschungsbereichs „Sichere Dinge“.

Andreas Koch ist seit 2005 Professor an der TU Darmstadt und leitet das Fachgebiet „Eingebettete Systeme und ihre Anwendungen“. Er ist an den LOEWE-Zentren CASED und AdRIA beteiligt.

Sascha Mühlbach arbeitet seit 2009 als Doktorand im Themenbereich „Sicherheit in Hochgeschwindigkeitsnetzen“ am Center for Advanced Security Research Darmstadt.

Marc Stöttinger arbeitet auf einer DFG-geförderten Forschungsstelle am Fachgebiet „Integrierte Schaltungen und Systeme“ der TU Darmstadt und ist assoziiertes Mitglied am CASED.