Expedition in den Nanokosmos

Prozessoren sind in unserem täglichen Leben allgegenwärtig, sie sind der Motor digitaler Technik. Wir machen uns wenig Gedanken darüber, denn die Halbleiter arbeiten zuverlässig im Verborgenen. Denken wir doch darüber nach, stehen Leistungseigenschaften im Vordergrund: Vor wenigen Jahren hat man bei der Auswahl eines neuen Computers noch auf die Taktfrequenz des Prozessors und die Größe des verbauten Speichers geachtet. Aktuelle Smartphones und Tablets haben in etwa die gleiche Leistung wie die damaligen Computer – nur sind sie viel handlicher und bringen bereits eine Menge an Peripherie mit, zum Großteil direkt integriert in den Prozessor-Chip.

Ist dieser mächtige Prozessor-Chip ein Kaufkriterum? Die Antwort ist in den meisten Fällen ein klares „Nein". Was zählt sind die unmittelbar sichtbaren Kriterien. Die Qualität des Bildschirms, die Anzahl und Auflösung der Kameras, die Kapazität des Akkus und nicht zu vergessen das Design.

Der Grund für diese Entwicklung liegt darin, dass die Prozessoren inzwischen so leistungsfähig sind, dass sie nicht mehr kaufentscheidend sind. Doch das ist nur die eine Seite der Medaille. Datenschutz und Datensicherheit ist die Grundvoraussetzung für eine erfolgreiche Digitalisierung. Ein Mehr an Leistungsfähigkeit wird oft durch Abstriche bei der Sicherheitsarchitektur erkauft. Vertrauen wir darauf, dass durch die Komplexität und hohe Integrationsdichte des System-on-a-Chip mit Taktfrequenzen im Gigahertzbereich und Strukturgrößen im einstelligen Nanometerbereich Angriffspfade schwer zu finden sind? Was tun wir, wenn es doch passiert?

Hardware ist keine Software und Updates sind in vielen Fällen konstruktionsbedingt nicht oder nur eingeschränkt über die Firmware möglich. Wir müssen mit Sicherheitslücken in Halbleitern leben und die Angriffsfläche nach Möglichkeit minimieren – oder wir produzieren Elektroschrott im großen Stil.

Faktisch wird die Komplexität, besser Obskurität, von Halbleitertechnologien ganz bewusst zur Umsetzung von ausgewiesenen und zertifizierten Sicherheitsfunktionen genutzt. Für die Verarbeitung von sensitiven Daten ist Kryptographie genauso unerlässlich, wie für die Identifikation oder Authentisierung. Moderne kryptographische Verfahren folgen dem Kerckhoffs'schem Prinzip, welches Auguste Kerckhoffs in *La cryptographie militaire* bereits 1883 formuliert hat: Die Sicherheit eines kryptographischen Verfahrens soll auf der Geheimhaltung des Schlüssels, nicht auf der Geheimhaltung des Algorithmus beruhen. Wozu also Obskurität, wenn die kryptographischen Verfahren öffentlich bekannt und gut untersucht sind? Zur Geheimhaltung der Schlüssel!

In diesem Schwerpunktheft begeben wir uns auf eine Expedition in den Nanokosmos der Halbleitertechnologie. Als Ihr Reiseleiter kann ich Ihnen versprechen, dass sich nicht alles auf den ersten Blick erschließen wird. Zunächst geht es auf Seitenkanälen zur Grenze des Nanokosmos. Nach der Prüfung Ihres Reisepass-Chips werden wir das eine oder andere Schreckgespenst beobachten können. Weiter geht es mit den Trojanischen Pferden über den Weg der Lieferkette. Dort schauen wir einem Titanen bei seinem Kampf gegen die Obskurität zu. Nach der Sicherung der Grundaufzeichnungen kommen wir zurück in die reale Welt. Mit Zielkonflikten zwischen Datenschutz und IT-Sicherheit sowie der Novellierung des Post-Datenschutzes beenden wir diese Expedition.

Ich wünsche eine aufregende Reise!

Dennis Kügler[1]

1 Dr. Dennis Kügler, Referatsleiter, Referat TK 11 – Sichere Halbleiter-Technologien, Bundesamt für Sicherheit in der Informationstechnik | E-Mail: dennis.kuegler@bsi.bund.de