Hardware-Sicherheit

Nicht erst seit den Abhörskandalen im Umfeld der Geheimdienste und den vermehrten Berichten über Sicherheitsvorfälle in der Tagespresse sollte jedermann, speziell aber den Anbietern und Betreibern von IT-Systemen, klar sein, dass Sicherheit in IT- bzw. IKT-Systemen in unserer Kommunikations- und Informationsgesellschaft unverzichtbar ist. Unabhängig vom Einsatzzweck verwenden kryptographische Mechanismen zur Gewährleistung von Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit kryptographische Schlüssel. Diese Schlüssel sollen in der Regel die wesentliche Hürde darstellen, die den Angreifer am Zugriff auf geschützte Daten und Informationen hindert. Kryptographische Schlüssel stellen daher ein attraktives Angriffsziel dar und sind somit vor unberechtigten Zugriffen bestmöglich zu schützen.

Werden Mechanismen wie Datenverschlüsselung oder digitale Signaturen auf einem PC, Laptop oder Smartphone genutzt, so werden die Daten, die Algorithmen und die kryptographischen Schlüssel zunächst in den Hauptspeicher geladen, um dann innerhalb der CPU verarbeitet zu werden. Die besonders kritischen Daten – insbesondere die kryptographischen Schlüssel – liegen dabei (wenn auch nur kurzfristig) im Klartext vor und sind prinzipiell durch Unbefugte auslesbar. Durch den Einsatz von geeigneter und besonders gesicherter Hardware kann das Schutzniveau der genutzten Schlüssel (und auch der eingesetzten Algorithmen) jedoch deutlich erhöht werden.

In diesem Heft wird sicherheitsrelevante Hardware aus unterschiedlichen Blickwinkeln betrachtet. Dabei wird der Bogen von den Einsatzszenarien von Hardware Security Modulen (HSM) über den Schutz der in solchen oder ähnlichen Produkten verbauten Komponenten, Seitenkanalangriffen auf Hardware (insbesondere Chipkarten) bis hin zur Sicherheitsbewertung und zur Absicherung eingebetteter (sicherheitskritischer) Systeme, gespannt.

Natürlich ist ein einzelner Baustein alleine nicht ausreichend, um IT-Sicherheit umfassend zu etablieren, aber zusammen mit den organisatorischen, personellen aber auch algorithmischen Maßnahmen stellen spezielle Hardwarekomponenten als so genannter „Sicherheitsanker" ein wesentliches Hilfsmittel für die Absicherung bestehender und zukünftiger IKT-Systeme dar.

Stefan Rass und Peter Schartner
E-Mail: {stefan | peter}@syssec.at