Sicherheits-ICs: Echter Schutz nur per Hardware

Alfred Vollmer ***Wer echte Sicherheit will und dabei nur auf Software setzt, der lässt entscheidende Sicherheitslücken offen. Nur eine spezielle Sicherheits-Hardware sorgt dafür, dass Hackern mit trojanischen Pferden und anderen unerwünschten Aktivitäten den sensiblen Daten nichts anhaben können. Soll gar ein Datenaustausch über das Internet erfolgen, dann gibt es bei nüchterner Betrachtung keine Alternative zu den Sicherheits-ICs. Wenn heutzutage das Thema auf in der Hardware verwurzelte Sicherheit kommt, denken die meisten Menschen nur an Chipkarten, doch das Thema ist weitaus vielschichtiger und die Einsatzgebiete dieser Sicherheits-Hardware reichen vom PC über die Kommunikations-Endgeräte bis zur Industrieelektronik.***

Homebanking per PC ist für viele heute bereits eine Selbstverständlichkeit. Da die persönlichen Daten verschlüsselt übertragen werden (https) denken viele, dass niemand z. B. die Kommunikation mit der Bank oder mit dem Online-Versand abhören kann. Doch trotz immer länger werdender SSL-Schlüssel (SSL: Secure Socket Layer; das Verschlüsselungsverfahren von Netscape Navigator und Microsoft Internet Explorer) ist es bei genauerer Betrachtung um die Datensicherheit ziemlich schlecht bestellt.

Der Grund dafür liegt in der Verschlüsselung per Software im PC-Prozessor. Das schöne an einem Computer ist die freie Programmierbarkeit, was auch zum großen Markterfolg der PCs führte. In der Praxis heißt das, dass jeder den PC so programmieren kann, wie er es gerne hätte – entsprechende Fachkenntnis einmal vorausgesetzt. Der Nachteil dieser universellen Programmierbarkeit ist die Möglichkeit, Programme laufen zu lassen, von denen der Anwender oft gar keine Ahnung hat. Man denke in diesem Zusammenhang nur an die vielen Viren und trojanischen Pferde.

Und genau hier liegt das Problem. Zwar kann man z. B. den Private-Key verschlüsselt speichern, aber während der Rechenoperationen im PC-Prozessor (Pentium, Athlon etc.) muss der Schlüssel im Klartext vorliegen. Dazu muss er zunächst in einem per Software frei zugänglichen Register des Prozessors abgespeichert werden. Zumindest hier liegt die verwundbare Stelle der Software-Verschlüsselung, denn ein Hacker könnte den Schlüssel aus dem PC auslesen und unbefugterweise nutzen. Wenn ein Hacker erst einmal über diesen Schlüssel verfügt, dann kann er die Informationen schon von außerhalb des Systems abfangen und entschlüsseln.

Spätestens der Virus *I Love You* hat gezeigt, wie leicht sich PCs manipulieren lassen. Was nutzen Hochsicherheitsschlösser an der Tür (Verschlüsselung), wenn man ein Fenster im Erdgeschoss geöffnet lässt (Schlüssel im PC-Prozessor verarbeiten)?

Verschlüsselung per Hardware

Aus diesem Grund ist für eine sichere Verschlüsselung eine separate Verschlüsselungs-Hardware nötig. Während bei der Verschlüsselung per Software der Schlüssel zu den Daten bzw. zum PC-Prozessor gebracht wird, transportiert man bei der Hardware-Verschlüsselung die Daten zum in einer speziellen Sicherheits-Hardware abgelegten Schlüssel. Dadurch hat niemand Zugriff auf den Schlüssel, weil dieser zu keinem Zeitpunkt in irgend einem per PC-Software erreichbaren Teil des PCs vorhanden ist. Erst hierdurch kann echte Sicherheit erreicht werden, die auch mit PC-Viren oder trojanischen Pferden nicht unterlaufen werden kann. Zusätzlich spielen besonders in Hochvolumenapplikationen, wie z. B. in Servern, Performance-Aspekte eine große Rolle. Diese geforderte Performance kann häufig nur durch zusätzliche Hardware erfüllt werden.

Bisher waren Sicherheits-ICs (Neudeutsch: Security-ICs) nur in Form von

Chipkarten bekannt. Von Infineon Technologies (gemeinsam mit ST Microelectronics dominiert Infineon seit Jahren den weltweiten Chipkarten-IC-Markt) kommen noch in diesem Jahr spezielle Security-ICs auf den Markt, mit denen Computer sicher werden können.
Je nach Anwendung hat man dabei derzeit die Auswahl unter verschiedenen Hardware-Lösungen, die direkt in die Rechner-Hardware integriert werden:

Bayon

Immer dann, wenn es darum geht, größere Datenmengen symmetrisch zu verschlüsseln, kommt der Bayon (SLD 9670) zum Einsatz, denn dieses IC sorgt nicht nur für lokale Sicherheit auf dem Rechner sondern auch für die nötige Netzwerksicherheit. Aufgrund seiner hohen Rechenleistung ist Bayon sogar in der Lage, sämtliche Daten, die auf die Festplatte geschrieben werden sollen, zu verschlüsseln bzw. die Daten beim Lesen wieder zu entschlüsseln, ohne dass dabei eine all zu große Verzögerung für den Benutzer spürbar wird.
Da Bayon über eine Funktion zum sicheren Auslesen von Chipkarten verfügt, kann der Computer-Anwender von einem kombinierten System aus Bayon und Chipkarte profitieren: Das in Bayon integrierte DES-Modul (DES: Data Encryption Standard) sorgt für eine sehr schnelle symmetrische Verschlüsselung der Daten, die über die PCI-Schnittstelle des ICs angeliefert bzw. wieder dem Rechner zur Verfügung gestellt werden. Die Chipkarte kommuniziert wiederum sicher mit Bayon und teilt diesem den aktuellen symmetrischen Schlüssel mit. Da die Kommunikation mit Chipkarten nur mit maximal etwa 150 Kbit/s möglich ist, kann die Chipkarte nicht selbst die Verschlüsselung der großen Datenmengen sinnvoll durchführen.
Mit diesem Verfahren verhält sich beispielsweise ein Notebook mit verschlüsselten Festplatten-Daten nach außen hin genau so wie ein Notebook ohne Verschlüsselungsfunktion – allerdings nur so lange die Chipkarte eingesteckt ist. Entfernt man die Chipkarte, so ist nicht nur der Notebook unbrauchbar. Auch die Daten auf der Festplatte lassen sich dann nicht mehr auslesen. So befinden sich beispielsweise auf den Festplatten der Notebook-Computer vieler Manager und Unternehmensberater oft äußerst sensible Daten, die auf gar keinen Fall in unbefugte Hände fallen dürfen. Wenn ein solcher Notebook auf einer der meist zahlreichen Geschäftsreisen abhanden kommt oder – wie in letzter Zeit häufiger vorgekommen – gezielt gestohlen wird, sind die Folgen oft kaum abschätzbar, falls die Daten nicht wirklich sicher auf der Festplatte verschlüsselt sind.
Bayon arbeitet am 32 bit breiten PCI-Bus, der mit 33 MHz getaktet wird. Er ermöglicht die symmetrische Verschlüsselung nach dem DES- bzw. Tiple-DES-Algorithmus mit 423 bzw. 141 Mbit/s. Zur Speicherung des Schlüssels stehen 128 Speicherplätze für Schlüssel, Signatur und Attribute zur Verfügung. Auch ein Sicherheits-Chipkarten-Controller aus der 66Plus-Familie ist bereits integriert. Zwei Chipkarten-Schnittstellen sowie ein UART- und ein GPI-Interface sind ebenfalls vorhanden.

TPM

Der TPM-Baustein entspricht den Anforderungen der TCPA (Trusted Computing Platform Alliance, Allianz für sichere/vertrauenswürdige Computer-Plattformen) an ein TPM (Trusted Platform Module, Modul für eine sichere/vertrauenswürdige Plattform). Das IC liefert Kommunikationspartnern Informationen über die Vertrauenswürdigkeit des PCs. Die prinzipielle Funktionsweise des TPM-ICs wurde von der TCPA mit dem Ziel definiert, den PC als vertrauenswürdige Plattform im Internet zu etablieren. Zu den Gründungsmitgliedern der TCPA zählen Intel, Microsoft, Hewlett-Packard, IBM und Compaq.
In seinem Innern verfügt der TPM-Chip unter anderem über einen nichtflüchtigen Speicher zum sicheren Aufbewahren von Schlüsseln. Er beherrscht die Verschlüsselungs-Standards DES sowie Triple-DES und erledigt eine RSA-Verschlüsselung mit 1024 bit in weniger als 300 ms. Ein Hash-Accelerator (SHA1, MD5) zur Integritätsprüfung sowie ein Zufallszahlen-Generator sind ebenfalls auf dem Chip integriert.

USB-Token

Bei dem USB-Token handelt es sich im wesentlichen um einen Chipkarten- ▶

„Sicherheit" ist für viele Anwender gleichbedeutend mit „Verschlüsselung", aber das Problem der Datensicherheit ist vielschichtiger. Im wesentlichen handelt es sich hierbei um vier generelle Aspekte:

1. Authentisierung
2. Datenintegrität
3. Vertraulichkeit und Geheimhaltung (Privacy)
4. Verfügbarkeit

1. Im täglichen Leben dient der Reisepass bzw. Personalausweis zur Identifizierung der Person. Im Computerbereich dienen derzeit vor allem Passwörter, aber auch vermehrt bereits Biometriedaten wie Fingerabdruck- oder Iris-Erkennung und Chipkarten als „Personalausweis". Ulrich Hamann, Leiter des Geschäftsbereichs Sicherheits- und Chipkarten-ICs sowie Leiter des Corporate Centers bei Infineon Technologies, definiert: „Die Chipkarte ist die Repräsentation eines menschlichen Wesens in einem technischen System."
2. Nachdem sich zwei Kommunikationspartner X und Y durch Authentisierungsmaßnahmen eindeutig identifiziert haben, muss sicher gestellt werden, dass exakt die Daten, die X an Y schickt, auch bei Y ankommen und umgekehrt. Die Kommunikationspartner müssen sich darauf verlassen können, dass die empfangenen Daten mit den ausgesandten Daten identisch sind. Sicherlich möchte niemand, dass beim Homebanking ein Hacker das Zielkonto und den Betrag manipuliert...
3. Hier kommt das klassische Thema Verschlüsselung zum tragen. Durch geeignete Verschlüsselungsmaßnahmen wird sicher gestellt, dass die vertraulichen Informationen in den abgehörten Datenströmen Dritten nicht zugänglich sind. Wenn beispielsweise ein Internet-Anwender A einem Online-Versandhaus Y seine Kreditkartendaten mitteilt, dann kann ein Hacker Z zwar die physikalisch übertragenen Daten abhören, aber bei geeigneter Verschlüsselung nicht entschlüsseln, so dass die gesamte Abhörmaßnahme nicht von Erfolg gekrönt ist.
4. Ein weiterer nicht zu unterschätzender Sicherheitsaspekt ist die Verfügbarkeit, denn wir sind mittlerweile von den Datennetzwerken so abhängig wie von der Stromversorgung. Auch wenn eine Netzwerkverbindung nur kurze Zeit gestört ist, kann dies doch gewaltige Folgen haben. Wenn der Kunde einer Online-Bank beispielsweise seine Aktiengeschäfte nicht zum gewünschten Zeitpunkt tätigen kann, dann kann das zu herben finanziellen Verlusten führen und wenn ein Internet-Versandhaus durch eine Netzwerkstörung von seinen Kunden abgeschnitten ist, dann führt dies zu Einbußen durch fehlenden Umsatz. Allerdings hat dieser Aspekt nichts mehr direkt mit der Sicherheits-Hardware zu tun.

Controller. Dieser verfügt jedoch nicht wie bei der Chipkarte über die langsame serielle Schnittstelle (150 Kbit/s), sondern über eine schnelle USB-Schnittstelle, die mittlerweile an jedem (neuen) Computer vorhanden ist, so dass kein zusätzliches Lesegerät nötig ist.
Erst durch diese schnellere Schnittstelle ist es sinnvoll möglich, dass der PC oft auf die Sicherheitsfunktionen des Chips zurückgreift, die ihm vom USB-Token als eine Art Sicherheitsdienstleistung angeboten werden. Wenn ein PC einen Schlüssel generieren will oder eine SSL-Session aufbauen will, dann muss er das nicht mehr auf der unsicheren PC-Plattform (z.B. im frei programmierbaren/zugänglichen Pentium-Prozessor) per Software erledigen, sondern er kann auf die Hardware-Sicherheit des USB-Token zurückgreifen.
Durch die Nutzung der 12 Mbit/s schnellen, überall vorhandenen USB-Schnittstelle lässt sich die hohe Sicherheit der Hardware-Verschlüsselung somit ohne zusätzliche Kosten (vom reinen USB-Token einmal abgesehen) erzielen. Da die USB-Schnittstelle für den Anwender zugänglich ist, gestaltet sich auch die Bedienung für den Computernutzer problemlos. Auch der USB-Token erledigt eine RSA-Verschlüsselung mit einem 1024 bit langen Schlüssel innerhalb von weniger als 300 ms.

Weiter technische Infos finden Sie im Internet:
www.trustedpc.org
www.silicon-trust.com

372 INFINEON

Alfred Vollmer *ist Redakteur der elektronik industrie. Dieser Beitrag basiert auf Informationen von Infineon Technologies.*