OHNE SECURITY GEHT NICHTS MEHR

Im Internet of Things und der Industrie 4.0 wird alles mit allem vernetzt sein. Das schafft neue Angriffspunkte für Spionage und Manipulationen. Daher müssen Systemdesigner Security in den Mittelpunkt neuer Entwicklungen stellen.

TEXT: Harald Maier, TQ-Group **BILDER:** TQ-Group; 123RF.com/Weerapat Kiatdumrong

Die Erfolgsgeschichte von Embedded-PC-Systemen begann vor vielen Jahren. Eine entscheidende Rolle spielte dabei die Standardisierung sowie die Kompatibilität und Austauschbarkeit in Sachen Hardware und Software. Bestehende Baugruppen und Schaltungsteile, ebenso wie Softwarefunktionen und Applikationen, werden wiederverwendet, was Entwicklungskosten und -zeiten reduziert. Jedoch eröffnen heute genau diese Vorteile auch die größten Angriffspunkte für bösartige Attacken, Missbrauch, Manipulation, Know-how-Diebstahl und Plagiate. Das IoT (Internet of Things), beziehungsweise die vernetzte Zukunft, verschärft die Problematik zunehmend.

Security – ein Muss für neue Entwicklungen

IoT ist in aller Munde und gibt Anlass, über Themen wie Security noch bewusster nachzudenken. In der vernetzten Zukunft gibt es diverse Kommunikationswege sowie eine Vielzahl von Schnittstellen und Standards. Die Anbindung ans Internet öffnet zudem eine neue Art der Zugänglichkeit. Damit einhergehend tun sich auch etliche neue Angriffspunkte für unbefugten Zugriff, Piraterie und Missbrauch auf. Gerade das hält viele Unternehmen davon ab, in das neue Zeitalter durchzustarten. Die Angst vor Spionage und Manipulation ist riesig. Sensible Daten, aber vor allem auch die Systeme selbst, benötigen ausreichenden Schutz. Optimal aufeinander abgestimmte Pakete aus Hardware und Software können dabei Risiken bestmöglich minimieren.

Bisher eingesetzte Systeme und Infrastrukturen waren zur Außenwelt hin gut abgeschottet und deshalb oft nur schwach oder gar nicht abgesichert. Sensible Daten, sowohl Nutzdaten wie auch spezielle Anwendungsprogramme, Algorithmen und Lizenzen, wurden im System oder in lokalen Netzen gespeichert und verwaltet. Auch die Systeme selbst hatten kaum Angriffspunkte in Bezug auf Manipulation oder Piraterie. Um ein System bösartig lahmzulegen, bedurfte es dem direkten Zugriff vor Ort. Spezielles Know-how auf Systemebene wurde oft durch eine Kombination aus proprietären Hardware-Komponenten und eigens dafür entwickelten Anwendungen umgesetzt und konnte so nur schwer abgekupfert werden.

Zugriffsmöglichkeiten auf Systeme und Daten haben sich gewandelt. Auch schützenswertes Know-how steckt immer mehr in den oberen Anwendungsschichten und somit verstärkt im Bereich der Software. Der Wunsch nach Update- und Servicemöglichkeiten benötigt neue Konzepte und Zugangsmöglichkeiten. Der Anspruch an flexible Nutzungs- und Lizensierungsmodelle bedarf neuer Mechanismen, um diese zu verwalten. Alles in allem werden Systemdesigner und Entwickler vor neue Herausforderungen gestellt. Bei allen spielt das Thema Security eine entscheidende Rolle. Nicht nur getrieben vom IoT und Industrie 4.0 besteht deshalb die Notwendigkeit, bei neuen Entwicklungen das Thema Security in den Mittelpunkt zu stellen.

Embedded-PC mit Multi-Level-Security

Embedded-PC-Technologie ist vielseitig einsetzbar und deckt durch die Flexibilität bei Erweiterungen, die Software-Kompatibilität und die Verfügbarkeit unterschiedlichs-

Abbildung 1: Sicherheit spielt eine zentrale Rolle bereits bei der Produktdefinition wie auch bei der Entwicklung und ist mitunter ausschlaggebend für den Produkterfolg.

ter Leistungsklassen vielfältige Anwendungsgebiete ab. Das Spektrum reicht vom intelligenten IoT-Gateway bis hin zu High-Performance-Rechnern für anspruchsvolle Automatisierungsaufgaben. Oft sind Embedded-PC-Anwendungen auch in der Medizintechnik zu finden. Gerade dort treffen Anforderungen an Sicherheit auf unterschiedlichsten Leveln zusammen. Es muss der Schutz sensibler Daten, der Schutz vor Manipulation und der Schutz des Applikations-Know-hows, eine flexible Lizensierung von Zusatzoptionen, die meist als Softwarefeatures implementiert sind, und die sichere Kommunikation mit der Umgebung gewährleistet sein.

Nur wenn der Aspekt Security bereits während der Entwicklungsphase berücksichtigt wird beziehungsweise Embedded-PC-Komponenten eingesetzt werden, die die notwendigen Sicherheits-Komponenten und -Mechanismen schon mit sich bringen, kann das System den heutigen Anforderungen gerecht werden.

Sollen Daten und Programme verschlüsselt auf einem lokalen Laufwerk abgelegt werden, so können Funktionen wie Bitlocker von Microsoft – verfügbar seit Windows 7 – eingesetzt werden. Diese Tools greifen auf Hardwarekomponenten wie den TPM-Baustein (Trusted Platform Module) zu, um die für die Entschlüsselung genutzten Schlüssel zu versiegeln. Die Daten sind nur für autorisierte Anwender verfügbar. Die Verschlüsselung ist gleichzeitig an das Gerät gebunden, sodass Hacker selbst durch Ausbau und Transfer der Festplatte/SSD in ein anderes System keine Kennwörter oder Daten auslesen können.

Zusätzlich kann ein im System integrierter TPM-Baustein auch für eine verschlüsselte Kommunikation und die eindeutige Identifizierung der Hardware in übergeordneten Systemen verwendet werden. TPMs können darüber hinaus genutzt werden, um Manipulation an Hardware und Software zu erkennen und darauf basierend einen sogenannten Secure-Boot oder Roots-of-Trust zu implementieren. TPMs können nicht nachgerüstet werden, da zusätzlich zum Hardware-Baustein auch die notwendigen Funktionen im BIOS (Basic Input/Output System) implementiert sein müssen.

Know-how schützen

Ein immer größerer Anteil des Know-hows liegt in der Software, was diese zu einem beliebten Ziel für Hacker und Reverse Engineering macht. Der Zugriff darauf wird bei schwach abgesicherten Systemen durch die immer stärkere Vernetzung wesentlich erleichtert. Ist die Kern-Software einmal extrahiert oder der Lizenzschlüssel geknackt, kann die Software ganz oder in Teilen auf andere Systeme übertragen und dort wiederverwendet werden. Einzelne Algorithmen und Spezial-Funktionen können mit Reverse-Engineering aus ungeschütztem Programm-Code extrahiert und in eigene Anwendungen integriert werden. Ein enormer Schaden, den es zu verhindern gilt. Schutz können hier sogenannte Security Controller bieten, die fest verlötet in das System integriert werden. Besonders schützenswerte Funktionen, meist reichen kleine Code-Blöcke, werden dabei beim Kompilieren so verschlüsselt, dass sie später nicht in der eigentlichen CPU, sondern nur auf dem dedizierten Security Controller des Zielsystems

Abbildung 2: Ein Beispiel für die Implementierung aller grundlegenden Security-Merkmale zeigt die Medical-PC-Plattform von TQ: TPM-Support, Security Controller und Wireless-Optionen, die eine sichere Kommunikation und umfassenden Schutz ermöglichen.

ausgeführt werden können. Die Software ist also nur auf dem dafür vorgesehenen Zielsystem lauffähig. Die verschlüsselten Programm-Code-Blöcke können so auch nicht während der Laufzeit getrackt und reverse-engineered werden.

Gleiches gilt für optionale Zusatz-Features, die per Lizenz freigeschaltet werden können. Wird die Aktivierung rein per Software realisiert, so ist es meist nur eine Frage der Zeit und des Aufwands, bis die notwendigen Lizenz-Strings oder Freischaltroutinen geknackt sind. Für einen sicheren Schutz müssen Hardware und Software aufeinander abgestimmt sein und Lizenzfreischaltungen (Lizenzschlüssel und Freischaltroutinen) beispielsweise in die bereits oben erwähnten Security Controller ausgelagert werden. Ähnliches ist bekannt aus dem Endanwenderbereich von sogenannten Hardware-Dongles, die am USB-Port eingesteckt werden. Bei Embedded-PC-Systemen ist es jedoch ratsam, diese mit fest integrierten Chips zu realisieren, sodass eine feste Zuordnung zum Gerät oder System gewährleistet ist. Nur wenn dies schon in der Entwicklungsphase vorgesehen wurde, können sichere Lizensierungsverfahren implementiert und das Know-how und kostenpflichtige Zusatzoptionen vor Missbrauch entsprechend geschützt werden.

Hemmungen vor vernetzter Zukunft ablegen

Kabelgebundene Kommunikation erfolgt meist innerhalb von lokalen Netzwerken oder innerhalb von IT-Infrastrukturen, die zur Außenwelt hin gut über Firewalls und ähnliches geschützt sind. Erfolgt die Kommunikation per Funkstandards, so ist ein erhöhtes Risiko gegeben. Vor allem dann, wenn der Kommunikationsweg direkt ins Internet führt. Speziell im Bereich zellularer Kommunikation (2G/3G/LTE), die genutzt wird, um ganzheitliche IoT-Lösungen aufzubauen, ist bei der Auswahl der Kommunikationskomponenten darauf zu achten, welche Sicherheitsfeatures bereits integriert sind. Schon bei der Entwicklung sollte die gesamte Kommunikationskette betrachtet werden: vom System bis zur Cloud. Hier ist es meistens von Vorteil, auf Hersteller zu setzen, die Kommunikationsmodule mit passenden Software-Routinen für die Cloud-Anbindung sowie die Cloud-Services selbst aus einer Hand anbieten.

Gerade wenn es um neue Anwendungen im IoT-Bereich und die vernetzte Zukunft geht, gibt es oft Unsicherheiten und Hemmungen, weil das Thema Sicherheit schwer einzuschätzen ist. Security spielt eine zentrale Rolle und muss als Basisanforderung schon während der Produktdefinitionsphase und Entwicklung berücksichtigt werden. Um Erfahrungslücken zu schließen und offene Fragen zu klären, kann es eine clevere Vorgehensweise sein, Partner mit einzubinden und bereits bestehende Plattformen zu nutzen. Das kann sowohl auf Komponentenebene als auch auf Systemebene erfolgen.

Weitere Informationen zu TQ-Systems finden Sie im Business-Profil auf Seite 72.