Segger schützt Firmware

Produzieren lassen ohne Trittbrettfahrer

23. Juni 2017, 08:46 Uhr | Von Dirk Akemann

Flasher Secure schützt Firmware for Produktpiraterie.

Mit den Chancen in den Bereichen Industrie 4.0 und Internet of Things wachsen auch die Anforderungen an die Produktion. Wie lässt sich sicherstellen, dass meine Geräte wirklich nur für mich produziert werden?

Mit der Globalisierung der Produktentwicklung entstehen völlig neue Chancen aber auch Risiken. Auf der Chancen-Seite besteht die Möglichkeit, die eigenen Produktionskapazitäten mit Hilfe von externen Fertigern bzw. Contract Manufacturers (CM) zu erweitern oder gar komplett an diese auszulagern. Auf der anderen Seite entsteht dadurch das Risiko, dass man dem Auftragsfertiger Firmengeheimnisse bzw. die eigene Intellectual Property (IP) offenlegen muss, damit dieser überhaupt in der Lage ist, die Produktion zu übernehmen.

Neben der Ausbaugeschwindigkeit der Produktion spielt damit noch ein weiterer Faktor für das Wachstum eine gewichtige Rolle: Der Contract Manufacturer muss verantwortlich und vertrauensvoll mit dem IP des Auftraggebers umgehen und darf nicht auf eigene Rechnung zusätzliche Geräte produzieren. Wie konkret dieses Szenario ist, wurde einem Spielzeughersteller schmerzlich bewusst. Dieser hatte Contract Manufacturers beauftragt, 1 Million elektronischer Spielzeuge herzustellen. Als er die elektronischen Spielzeuge aus verschiedenen Gründen zurückrufen musste, bekam er 1,8 Millionen davon zurück, also mindestens 800.000, die er selbst weder hergestellt noch beauftragt hatte. Offenbar haben Contract Manufacturers mindestens 800.000 elektronische Spielzeuge auf eigene Rechnung produziert und verkauft.

Schlüsselelement Firmware

Für jeden verantwortungsvollen Auftraggeber ist es zwingend notwendig sicherzustellen, dass die Weitergabe seines IPs an den Contract Manufacturer nicht missbraucht werden kann. Dabei kommt ihm in der Regel zugute, dass der überwiegende Teil der Innovation heutzutage in der Firmware steckt. Um sein geistiges Eigentum zu schützen, muss sich der Auftraggeber insbesondere um den Schutz der Firmware kümmern.

Allein die Programmierung der Firmware on-site, also in der eigenen kontrollierbaren Umgebung durchzuführen, ist kein ausreichender Schutz gegen Cloning. Die Hardware nachzubauen und die Firmware zu kopieren gehört in gewissen Kreisen zum Basiswissen. Sicher, auf der einen Seite kann man es als Auszeichnung werten, wenn man so erfolgreich ist, dass andere sich um den Nachbau bemühen, auf der anderen Seite hat der Diebstahl geistigen Eigentums erhebliche Verluste für den Auftraggeber zur Folge. Um den Nachbau so teuer wie möglich und damit unrentabel oder unmöglich zu machen, kann sich der Auftraggeber aus verschiedenen Angeboten bedienen. Viele der Angebote berücksichtigen aber entweder nicht die besonderen Gegebenheiten von Mikrocontroller-Systemen oder müssen selbst zusammengebaut und gepflegt werden. Eine Möglichkeit, dies zu verhindern, bieten Authentifizierungsalgorithmen an. Mit digitalen Signaturen wird dabei festgestellt, ob das vorliegende Gerät auch tatsächlich vom ursprünglichen Hersteller stammt. Die Firma Segger bietet eine solche Lösung an. Das Authentifizierungsverfahren wird mit dem Produkt emSecure auch den Kunden von Segger verfügbar gemacht, sodass diese das erprobte Verfahren für ihre eigenen Produkte anwenden können.

Für die Programmierung der Signaturen wird ein zusätzlicher Prozess in der Produktion installiert. Der Prozess besteht darin, dass das Produktionssystem eindeutige Identifikationsdaten aus dem zu programmierenden Gerät ausliest, diese mit dem firmeneigenen privaten Schlüssel signiert und die erzeugte Signatur dann im Gerät abspeichert. Damit haben dann Bootloader, Firmware und auch externe Programme die Möglichkeit, die Authentizität der Hardware zu prüfen (**Bild 1**).

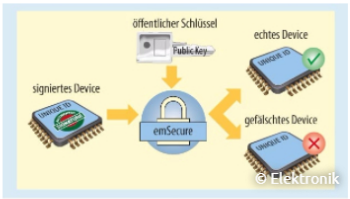

Bild 1. Flasher Secure verwendet für die Authentifizierung emSecure. emSecure ist sowohl als RSA- als auch als ECDSA-Version verfügbar.

Die Bilder des Artikels im Überblick, Bilder 1-3