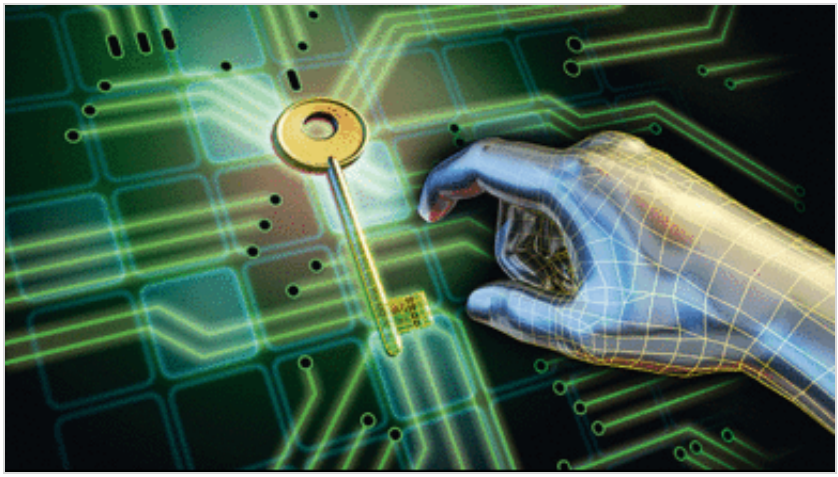
Security:

Gut geschützt vor Hackern und Klonern

02.07.2015 Von Joachim Kroll

Digitale Signaturen schützen vor Hacker-Angriffen und machen das Klonen von Produkten nahezu unmöglich. Das Software-Paket emSecure ist eigens für den Einsatz von Signaturen auf Embedded-Systemen ausgelegt.



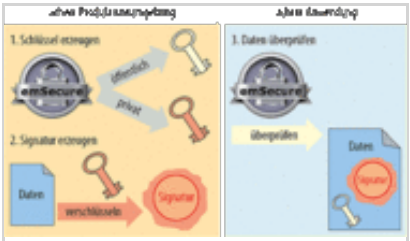
© Andrea Danti - Fotolia

Je mehr das Internet of Things Realität wird und Mikrocontroller Einzug in alltägliche Produkte und Anwendungen halten, desto mehr werden sie zur Zielscheibe von Hackern. Mit den Angriffen können unterschiedliche Ziele verbunden sein: der Diebstahl sensibler Daten, die Manipulation der Geräte oder der Diebstahl der Geräte-Software zum Zweck der Produktpiraterie. Doch dagegen gibt es ein Mittel: digitale Signaturen. Die Software emSecure von Segger Microcontroller [1] erzeugt solche Signaturen auf der Basis des etablierten RSA-Verfahrens. Dieses Verfahren wird beispielsweise auch zur Authentifizierung bei der Online-Steuererklärung (Elster) verwendet. Mit Hilfe von RSA wird ein Schlüsselpaar (Public Key und Private Key) generiert, das bei entsprechender Schlüssellänge nicht voneinander abgeleitet werden kann.

Schlüssellängen von 2048 bit können bislang nicht geknackt werden und es ist nach übereinstimmender Expertenmeinung auch nicht davon auszugehen, dass dies in den kommenden Jahrzehnten gelingt. emSecure unterstützt Schlüssel bis zu einer Länge von 16.384 bit.

Schutz der Firmware

Im Kampf gegen Hacking setzt emSecure bei der Firmware an. Sie ist seit jeher das Einfallstor für Angriffe Dritter, weil sie meistens nicht unter dem Aspekt der Sicherheit aufgebaut ist. Die digitale Signatur verhindert, dass Dritte die Firmware und damit die Funktion des Mikrocontrollers manipulieren können. Dies funktioniert folgendermaßen: Der Hersteller eines Mikrocontroller-basierten Produktes generiert ein Schlüsselpaar und verankert den Public Key im Produkt. Firmware Updates für dieses Produkt werden dann mit einer digitalen Signatur versehen, die der Hersteller mit Hilfe seines Private Key erzeugt. Bei der Aktualisierung durch den Kunden wird automatisch mit Hilfe des Public Key geprüft, ob die Signatur verifiziert werden kann. Nur dann wird das Update auch aufgespielt. Nicht authentische Dateien werden abgelehnt.



© Segger

Mit Signaturen können z.B. Firmware-Updates auf Gültigkeit überprüft werden. Im Produkt befindet sich der öffentliche Schlüssel des

Herstellers. Ein Firmware-Update wird vom Produkt nur akzeptiert, wenn es mit dem privaten Schlüssel des Herstellers signiert wurde.

Dabei ist der Einsatz von emSecure so einfach und schnell, dass er weder den Entwicklungsprozess noch die Fertigung oder den Betrieb des Produktes im Feld beeinträchtigt. Selbst bei der Schlüssellänge von 2048 bit, die höchste Sicherheit gewährleistet, dauert die Authentifizierung einer Signatur nur 45 ms. Ermittelt wurde dieser Wert für einen typischen Cortex-M4-basierten Mikrocontroller mit 200 MHz. Der statische RAM-Bedarf für emSecure liegt bei Null, die Verifikation findet ausschließlich auf dem Stack statt.

Ein weiterer Einsatzbereich ist Anti-Cloning. Dafür wird das Originalgerät mit einer digitalen Signatur versehen, die auf einem einzigartigen Merkmal der Hardware beruht, z.B. der Unique ID, die viele Mikrocontroller besitzen. So kann die Firmware des Originalgerätes nicht einfach ausgelesen und in ein nachgebautes Gerät kopiert werden.

Solange man einen Standard-Mikrocontroller einsetzt, wird es für Hacker, die über enorme Ressourcen und Zeit verfügen, einen Weg geben, das Sicherheits-System temporär auszuschalten: Sie könnten ein solches Gerät analysieren und nachbauen, sodass schließlich der Klon-Check deaktiviert werden kann. Doch selbst wenn Raubkopierern ein solcher Nachbau gelungen ist: Spätestens wenn das erste authentische Firmware Update kommt, wird die Kopie enttarnt, denn dieses Update lässt sich aufgrund der fehlenden Signatur in der Geräte-Firmware nicht aufspielen.

Mit zusätzlichen Maßnahmen lässt sich das Sicherheitsniveau bei der Verwendung von digitalen Signaturen weiter erhöhen. So sollte der Rechner, mit dem der Private Key erzeugt wird, nur für diesen Zweck verwendet werden – idealerweise offline. Außerdem kann der Private Key verschlüsselt aufbewahrt werden.

Maßnahmen gegen Schlüsselverlust

Grundsätzlich können Keys auf zwei Wegen erzeugt werden: per Zufallsgenerator oder mit Hilfe einer Passphrase. Letzteres hat den Vorteil, dass sich die Keys immer wieder generieren lassen. Das könnte etwa notwendig werden, wenn der Private Key nicht mehr verfügbar ist. Entscheidet man sich für die Verwendung einer Passphrase, sollte diese aber nicht zu einfach zu erraten sein – der Firmenname wäre keine besonders sichere Wahl. Weiterhin kann der Signatur-Check auch an mehreren Stellen der Firmware verankert werden. Dies erschwert die vorübergehende Deaktivierung des Klon-Checks zusätzlich.

Das emSecure-Software-Paket enthält von der Schlüssel-Generierung bis zum Benchmarking der Verarbeitungsgeschwindigkeit verschiedener Schlüssellängen alle Module, die notwendig sind, um ein Produkt abzusichern – vorcompiliert und einsatzbereit. Ebenso sind Beispielanwendungen und der Quellcode enthalten. emSecure ist in ANSI-C geschrieben und nutzt keinen Code, der spezifisch ist für ein bestimmtes Betriebssystem oder bestimmte Hardware. Daher ist der Einsatzbereich praktisch unbegrenzt. Die Programmierschnittstelle ist sehr leistungsfähig, dabei gleichzeitig simpel. Die Integration in bestehende Produktionsumgebungen dauert weniger als einen halben Tag.

jk

Links im Artikel

1. http://www.elektroniknet.de/anbieterkompass/?anbieter=1057952